BENUTZERHANDBUCH

KASPERSKY INTERNET SECURITY 2009

Sehr geehrter Benutzer!

Danke, dass Sie sich für unser Produkt entschieden haben. Wir hoffen, dass Ihnen diese Dokumentation bei der Arbeit behilflich sein und auf die mit dem Produkt verbundenen Fragen antworten wird.

Der Inhalt des Dokuments kann zukünftig ohne besondere Ankündigung geändert werden. Die aktuelle Version des Dokuments steht auf der Seite von Kaspersky Lab unter der Adresse http://www.kaspersky.de/docs zur Verfügung. Kaspersky Lab übernimmt keine Haftung für Inhalt, Qualität, Aktualität und Richtigkeit von in diesem Dokument verwendeten Materialien, deren Rechte bei anderen Eigentümern liegen, sowie für möglichen Schaden, der mit der Verwendung dieser Materialien verbunden ist.

Tel.: +49 (0) 841 98 18 90
Fax: +49 (0) 841 98 189 100

http://www.kaspersky.de
http://support.kaspersky.com/de/

Erscheinungsdatum: 29.04.2008

INHALT

VORWORT ... 5
Suche nach Informationen über das Programm ... 5
Informationsquellen zur selbständigen Recherche ... 5
Kontaktaufnahme mit der Vertriebsabteilung ... 6
Kontaktaufnahme mit dem Technischen Support ... 6
Diskussion über die Programme von Kaspersky Lab im Webforum ... 8
Neuerungen in Kaspersky Internet Security 2009 ... 8
Schutzkonzeption der Anwendung ... 10
Assistenten und Werkzeuge ... 11
Servicefunktionen ... 12
Heuristische Analyse ... 13
Hardware- und Softwarevoraussetzungen ... 14

BEDROHUNGEN FÜR DIE COMPUTERSICHERHEIT ... 16
Bedrohliche Programme ... 16
Schädliche Programme ... 17
Viren und Würmer ... 17
Trojanische Programme ... 20
Schädliche Tools ... 27
Potentiell unerwünschte Programme ... 30
Adware ... 31
Programme mit pornografischem Charakter ... 31
Sonstige potentiell unerwünschte Programme ... 32
Wie die Anwendung infizierte, verdächtige und potentiell gefährliche Objekte erkennt ... 36
Internet-Bedrohungen ... 37
Spam oder unerwünschte eingehende E-Mail ... 37
Phishing ... 38
Hackerangriffe ... 38
Anzeige von Bannern ... 39

INSTALLATION DER ANWENDUNG AUF EINEM COMPUTER ... 40
Schritt 1. Suche nach einer neueren Programmversion ... 41
Schritt 2. Überprüfen des Systems auf die Installationsvoraussetzungen ... 42
Schritt 3. Startfenster des Installationsassistenten ... 42
Schritt 4. Lesen des Lizenzvertrags ... 42
Schritt 5. Auswahl des Installationstyps ... 43
Schritt 6. Auswahl des Installationsordners ... 43

Schritt 7. Auswahl der zu installierenden Programmkomponenten 44
Schritt 8. Suche nach anderen Antiviren-Programmen 45
Schritt 9. Abschließende Vorbereitungen für die Programminstallation 46
Schritt 10. Abschluss des Installationsvorgangs 46

PROGRAMMOBERFLÄCHE 48
Symbol im Infobereich der Taskleiste 48
Kontextmenü 49
Programmhauptfenster 51
Meldungen 54
Programmkonfigurationsfenster 54

ERSTE SCHRITTE 55
Auswahl des Netzwerktyps 56
Programm-Update 57
Sicherheitsanalyse 57
Virenuntersuchung des Computers 58
Teilnahme an Kaspersky Security Network 58
Sicherheitsverwaltung 59
Schutz anhalten 61

ÜBERPRÜFUNG DER PROGRAMMEINSTELLUNGEN 63
EICAR-"Testvirus" und seine Modifikationen 63
Testen des Schutzes für HTTP-Datenverkehr 67
Testen des Schutzes für SMTP-Datenverkehr 67
Überprüfung der Einstellungen von Datei-Anti-Virus 68
Überprüfung der Einstellungen für eine Aufgabe zur Virensuche 68
Überprüfung der Einstellungen für den Schutz vor unerwünschten E-Mails . 69

ERKLÄRUNG ZUR VERWENDUNG VON
KASPERSKY SECURITY NETWORK 70

KASPERSKY LAB 76
Andere Produkte von Kaspersky Lab 77
Unsere Kontaktinformationen 87

MOZILLA FOUNDATION 88

ENDBENUTZER-LIZENZVERTRAG FÜR DIE ERWORBENE KASPERSKY LAB
SOFTWARE 89

VORWORT

IN DIESEM ABSCHNITT

Suche nach Informationen über das Programm 5

Neuerungen in Kaspersky Internet Security 2009 8

Schutzkonzeption der Anwendung 10

Hardware- und Softwarevoraussetzungen 14

SUCHE NACH INFORMATIONEN ÜBER DAS PROGRAMM

Wenn Sie Fragen zu Auswahl, Kauf, Installation oder Verwendung der Anwendung haben, können Sie schnell eine Antwort darauf erhalten.

Kaspersky Lab bietet unterschiedliche Informationsquellen zu der Anwendung an, unter denen Sie abhängig von der Dringlichkeit und Bedeutung Ihrer Frage wählen können.

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Sie können das elektronische Hilfesystem verwenden.

Die Hilfe bietet Informationen darüber, wie der Computerschutz gesteuert wird: Anzeige des Schutzstatus, Untersuchung bestimmter Computerbereiche auf Viren, Ausführen anderer Aufgaben.

Um die Hilfe zu öffnen, klicken Sie im Programmhauptfenster auf den Link **Hilfe** oder verwenden Sie die Taste **<F1>**.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf des Programms sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung in unserer Zentrale in Moskau unter folgenden Telefonnummern zur Verfügung:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**.

Die Beratung kann auf Englisch oder Russisch erfolgen.

Sie können sich mit Ihrer Frage auch unter folgender Adresse per E-Mail an die Mitarbeiter der Vertriebsabteilung wenden: sales@kaspersky.com.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Wenn Sie die Anwendung bereits erworben haben, können Sie von den Spezialisten des Technischen Supports per Telefon oder über das Internet Informationen darüber erhalten.

Die Spezialisten des Technischen Supports beantworten Ihre Fragen zur Installation und Verwendung des Programms und helfen Ihnen dabei, die Folgen von Virenangriffen zu beheben, wenn Ihr Computer infiziert wurde.

Beachten Sie bitte die Support-Regeln, bevor Sie sich an den Technischen Support wenden (http://support.kaspersky.de/support/rules).

E-Mail-Anfrage an den Technischen Support (für registrierte Benutzer)

Sie können Ihre Frage den Spezialisten des Technischen Supports stellen. Füllen Sie dazu das Webformular aus, das sich auf der Seite für Kundenanfragen befindet (http://support.kaspersky.com/de/).

Die Anfrage kann in deutscher, englischer, französischer, spanischer oder russischer Sprache gestellt werden.

Um eine E-Mail-Anfrage zu stellen, ist die Angabe der **Kundennummer**, die Sie bei der Anmeldung auf der Webseite des Technischen Supports erhalten haben, und des **Kennworts** erforderlich.

> Hinweis
>
> Wenn Sie noch nicht als Benutzer eines Kaspersky-Lab-Programms registriert sind, können Sie das Anmeldeformular ausfüllen (https://support.kaspersky.com/de/PersonalCabinet/Registration/Form/). Geben Sie bei der Registrierung den *Aktivierungscode* des Programms oder den *Namen der Schlüsseldatei* an.

Die Spezialisten des Technischen Supports werden Ihre Frage in Ihrem **Personal Cabinet** (https://support.kaspersky.com/de/PersonalCabinet) und per E-Mail an die in der Anfrage angegebene Adresse beantworten**.**

Beschreiben Sie im Webformular das aufgetretene Problem möglichst genau. Machen Sie in den obligatorisch auszufüllenden Feldern folgende Angaben:

- **Typ der Anfrage**. Die Fragen, die häufig von Benutzern gestellt werden, sind in einer Liste vorgegeben. Dazu zählen beispielsweise: "Problem bei der Installation/Deinstallation des Produkts" oder "Problem bei der Suche/Desinfektion von Viren". Wenn keine der Kategorien zutrifft, wählen Sie den Punkt "Allgemeine Frage".
- **Name und Versionsnummer des Programms**.
- **Anfragetext**. Beschreiben Sie das Problem möglichst genau.
- **Kundennummer und Kennwort**. Geben Sie die Kundennummer und das Kennwort an, die Sie bei der Anmeldung auf der Webseite des Technischen Supports erhalten haben.
- **E-Mail-Adresse**. An diese Adresse werden die Support-Spezialisten Ihre Anfrage beantworten.

Technischer Support am Telefon

Zur Lösung dringender Probleme können Sie jederzeit den Technischen Support in Ihrer Umgebung anrufen. Wenn Sie den russischen (http://support.kaspersky.com/support/support_local) oder internationalen (http://support.kaspersky.com/de/support/international) Technischen Support um Hilfe bitten, geben Sie bitte die erforderlichen Informationen an (http://support.kaspersky.com/de/support/details). Dadurch ermöglichen Sie es unseren Spezialisten, Ihnen am schnellsten helfen.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse http://forum.kaspersky.com besprechen.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

NEUERUNGEN IN KASPERSKY INTERNET SECURITY 2009

Kaspersky Internet Security 2009 bietet ein prinzipiell neues Herangehen für den Schutz von Informationen. Einen wichtigen Aspekt in der Anwendung bildet die Beschränkung der Rechte von Programmen für den Zugriff auf Systemressourcen. Dadurch wird erlaubt, verdächtige oder gefährliche Programme daran zu hindern, unerwünschte Aktionen auszuführen. Die Programmfunktionen zum Schutz vertraulicher Benutzerdaten wurden wesentlich erweitert. Die Anwendung umfasst Assistenten und Werkzeuge, mit denen sich das Ausführen spezifischer Aufgaben zum Schutz Ihres Computers erheblich vereinfachen lässt.

Im Folgenden werden die Neuerungen in Kaspersky Internet Security 2009 ausführlich beschrieben.

Neuerungen im Schutz:

- Kaspersky Internet Security enthält die Komponente Aktivitätsfilterung, die im Verbund mit dem Proaktiven Schutz und der Firewall eine neue und umfassende Methode für den Schutz des Systems vor allen Bedrohungen realisiert. Dies bezieht sich sowohl auf bekannte als auch auf bisher unbekannte Gefahren. Die Anzahl der Anfragen von Kaspersky Internet Security an den Benutzer, wurde erheblich reduziert, was durch die Verwendung von Listen mit vertrauenswürdigen Anwendungen (Whitelisting) erreicht wird.
- Die Analyse von Schwachstellen im Betriebssystem und in Programmen und deren anschließende Behebung gewährleisten dem System ein hohes Sicherheitsniveau und verhindern das Eindringen schädlicher Programme auf den Computer.
- Die neuen Assistenten Sicherheitsanalyse und Browser-Konfiguration erleichtern die Suche und das Beheben von Sicherheitsrisiken und

Schwachstellen in den Anwendungen, die auf Ihrem Computer installiert sind, sowie in den Einstellungen des Betriebssystems und des Browsers.

- Die Reaktionsgeschwindigkeit von Kaspersky Lab auf neue Gefahren wurde durch die Verwendung der Technologie Kaspersky Security Network gesteigert (s. Abschnitt "Teilnahme an Kaspersky Security Network" auf S. 58). Dabei werden Daten über Infektionen von Benutzercomputern gesammelt und an die Kaspersky-Lab-Server gesendet.
- Die neuen Werkzeuge Netzwerkmonitor und Analyse von Netzwerkpaketen erleichtern das Sammeln und die Analyse von Informationen über die Netzwerkaktivitäten auf Ihrem Computer.
- Der neue Assistent zur Wiederherstellung nach Infektion hilft dabei, nach dem Angriff eines schädlichen Programms Beschädigungen am System zu beheben.

Neuerungen im Schutz für vertrauliche Daten:

- Die neue Komponente Aktivitätsfilterung kontrolliert auf effektive Weise den Zugriff von Anwendungen auf vertrauliche Daten, Dateien und Ordner des Benutzers.
- Das neue Werkzeug Virtuelle Tastatur bietet Sicherheit für vertrauliche Daten, die über die Tastatur eingegeben werden.
- Zum Lieferumfang von Kaspersky Internet Security gehört der Assistent zum Löschen von Aktivitätsspuren, der Informationen über die Aktionen des Benutzers vom Computer löscht, die für Angreifer interessant sein können (Liste der besuchten Webseiten, geöffneten Dateien, Cookies usw.).

Neuerungen im Schutz vor dem Empfang unerwünschter Daten:

- Die Effektivität der Filterung unerwünschter E-Mails durch die Komponente Anti-Spam wurde durch die Verwendung der Servertechnologien Recent Terms erhöht.
- Die Verwendung von Erweiterungsmodulen für die Mailprogramme Microsoft Office Outlook, Microsoft Outlook Express, The Bat! und Thunderbird vereinfacht die Konfiguration des Spam-Schutzes.
- Die optimierte Komponente Kindersicherung erlaubt es, den Zugriff von Kindern auf unerwünschte Internetressourcen sinnvoll zu beschränken.

Neuerungen im Schutz bei der Arbeit im Internet:

- Der Schutz vor Internetbetrügern wurde durch den Ausbau der Datenbanken für Phishing-Seiten verbessert.

- Eine Untersuchung des Datenverkehrs von ICQ und MSN wurde hinzugefügt. Dadurch wird die sichere Arbeit mit Internet-Messengern gewährleistet.
- Die Sicherheit bei der Arbeit in drahtlosen Netzwerken wird durch die Untersuchung von WiFi-Verbindungen erreicht.

Neuerungen auf der Programmoberfläche:

- Die neue Programmoberfläche spiegelt das komplexe Herangehen an den Informationsschutz wider.
- Die Dialogfenster bieten ein Höchstmaß an Informationen und unterstützen den Benutzer dabei, schnell die richtige Entscheidung zu treffen.
- Die Funktionalität der Berichte und statistischen Informationen über die Arbeit der Anwendung wurde erweitert. Die Möglichkeit zur Verwendung flexibel einstellbarer Filter bei der Arbeit mit Berichten macht das Produkt für Profis unersetzbar.

SCHUTZKONZEPTION DER ANWENDUNG

Kaspersky Internet Security bietet Ihrem Computer Schutz vor bekannten und neuen Bedrohungen, Hacker- und Betrugsangriffen, Spam und anderen unerwünschten Daten. Jeder Bedrohungstyp wird von einer einzelnen Anwendungskomponente verarbeitet. Dieser Aufbau des Schutzsystems erlaubt es, das Programm flexibel an die Erfordernisse eines konkreten Benutzers oder Unternehmens anzupassen.

Kaspersky Internet Security umfasst:

- Aktivitätskontrolle für Programme im System, die verhindert, dass Programme gefährliche Aktionen ausführen.
- Komponenten zum Schutz vor schädlichen Programmen, die Ihren Computer im Echtzeitschutz-Modus auf allen Kanälen schützen, über die Informationen empfangen und gesendet werden.
- Komponenten zum Schutz bei der Arbeit im Internet, die dazu dienen, Ihren Computer vor den bekannten Netzwerkangriffen und Betrugsversuchen zu schützen.
- Komponenten zur Filterung unerwünschter Daten, die Ihnen helfen, Zeit, Datenverkehr und Geld zu sparen.

- Aufgaben zur Virensuche, mit deren Hilfe die Virenuntersuchung in einzelnen Dateien, Ordnern, Laufwerken oder Bereichen, oder die vollständige Untersuchung des Computers ausgeführt wird. Die Untersuchungsaufgaben können so eingestellt werden, dass sie in den Anwendungen, die auf dem Computer installiert sind, Schwachstellen erkennen.
- Update, das den aktuellen Zustand der internen Programm-Module sowie der Datenbanken, die zur Suche nach schädlichen Programmen und zum Erkennen von Hackerangriffen und Spam-Mails verwendet werden, aufrechterhält.
- Assistenten und Werkzeuge, die es erleichtern, Aufgaben, die zur Arbeit von Kaspersky Internet Security erforderlich sind, auszuführen.
- Servicefunktionen, die Informationen über die Arbeit mit dem Programm bieten und es erlauben, die Programmfunktionalität zu erweitern.

ASSISTENTEN UND WERKZEUGE

Es ist keine einfache Aufgabe, die Sicherheit eines Computers zu gewährleisten. Dafür sind Kenntnisse über Besonderheiten der Funktion eines Betriebssystems und über potentielle Schwachstellen erforderlich. Zudem erschweren die große Menge und die Vielfalt der Informationen über die Systemsicherheit deren Analyse und Verarbeitung.

Um spezifische Aufgaben, die die Sicherheit des Computers gewährleisten, zu vereinfachen, verfügt Kaspersky Internet Security über unterschiedliche Assistenten und Werkzeuge.

- Der Assistent zur Sicherheitsanalyse führt eine Diagnose der Computersicherheit und eine Suche nach Schwachstellen im Betriebssystem und in Programmen, die auf dem Computer installiert sind, aus.
- Der Assistent zur Browser-Konfiguration führt eine Analyse der Parameter des Browsers Microsoft Internet Explorer aus und bewertet die Parameter im Hinblick auf die Sicherheit.
- Der Assistent zur Wiederherstellung nach einer Infektion beseitigt im System die Spuren von schädlichen Objekten.
- Der Assistent zum Löschen von Aktivitätsspuren sucht und beseitigt im System und in den Betriebssystemparametern die Aktivitätsspuren des Benutzers.
- Die Notfall-CD soll zur Wiederherstellung der Funktionsfähigkeit des Systems nach einem Virenangriff dienen, durch den Systemdateien des

Betriebssystems beschädigt wurden und der Computer nicht mehr hochgefahren werden kann.

- Die Analyse von Netzwerkpaketen fängt Netzwerkpakete ab und bietet ausführliche Informationen darüber.
- Der Netzwerkmonitor bietet detaillierte Informationen über die Netzwerkaktivitäten auf Ihrem Computer.
- Die virtuelle Tastatur ermöglicht es, das Abfangen von über die Tastatur eingegebenen Daten zu verhindern.

SERVICEFUNKTIONEN

Die Anwendung verfügt über eine Reihe von Servicefunktionen. Sie dienen dazu, den aktuellen Zustand der Anwendung aufrechtzuerhalten, die Funktionen der Anwendung zu erweitern und bei der Arbeit Hilfe zu bieten.

Kaspersky Security Network

Kaspersky Security Network ist ein System, das automatisch Berichte über gefundene und potentielle Bedrohungen an eine zentrale Datenbank überträgt. Diese Datenbank erlaubt es, schneller auf weit verbreitete Gefahren zu reagieren und die Benutzer über Epidemien zu informieren.

Lizenz

Beim Kauf der Anwendung wird zwischen Ihnen und Kaspersky Lab ein Lizenzvertrag abgeschlossen, auf dessen Grundlage Sie die Anwendung verwenden dürfen und für einen festgelegten Zeitraum Zugriff auf Updates für die Datenbanken der Anwendung und auf den Technischen Support-Service erhalten. Die Nutzungsdauer sowie andere Informationen, die zur vollfunktionalen Arbeit der Anwendung erforderlich sind, sind in der Lizenz angegeben.

Mit der Funktion **Lizenz** können Sie ausführliche Informationen über die von Ihnen verwendete Lizenz erhalten. Außerdem können Sie damit eine neue Lizenz erwerben oder die Gültigkeit der aktiven Lizenz verlängern.

Support

Alle registrierten Benutzer der Anwendung können den Technischen Support-Service in Anspruch nehmen. Verwenden Sie die Funktion **Support**, um zu erfahren, wo Sie technische Unterstützung erhalten können.

Mit Hilfe der entsprechenden Links gelangen Sie zum Benutzerforum für die Kaspersky-Lab-Produkte und können auf der Webseite ein spezielles Formular ausfüllen, um eine Fehlermeldung oder eine Rückmeldung über die Arbeit des Programms an den Technischen Support-Service zu senden.

Zusätzlich stehen Ihnen der Online-Service des technischen Kundendiensts und die Dienste für das Personal Cabinet des Benutzers zur Verfügung. Natürlich können Sie sich auch telefonisch an unsere Mitarbeiter wenden, um bei der Arbeit mit der Anwendung Hilfe zu erhalten.

HEURISTISCHE ANALYSE

Heuristische Analysemethoden werden bei der Arbeit verschiedener Echtzeitschutz-Komponenten wie z.B. in Datei-Anti-Virus, Mail-Anti-Virus und Web-Anti-Virus sowie in Aufgaben zur Virensuche verwendet.

Es ist bekannt, dass die Untersuchung durch die Signaturmethode mit zuvor erstellten Datenbanken, die eine Beschreibung bekannter Bedrohungen und entsprechende Desinfektionsmethoden enthalten, eine eindeutige Antwort darauf gibt, ob ein Objekt schädlich ist und zu welcher Malware-Klasse es gegebenenfalls gehört. Im Unterschied zur Signaturmethode orientiert sich die heuristische Methode bei der Suche nach Bedrohungen nicht an Malware-Signaturen, sondern an typischen Operationsfolgen, die mit hinreichender Wahrscheinlichkeit eine Schlussfolgerung über die Art einer Datei zulassen.

Der Vorteil der heuristischen Analyse besteht darin, dass für ihre Arbeit keine zuvor erstellten Datenbanken benötigt werden. Dadurch können neue Bedrohungen bereits erkannt werden, bevor die Virenanalytiker von ihrer Aktivität wissen.

Allerdings existieren Verfahren, mit denen heuristische Methoden überlistet werden können. Ein Trick besteht darin, die Malware-Aktivität anzuhalten, sobald bemerkt wird, dass heuristische Untersuchungsmethoden verwendet werden.

> Hinweis
>
> Durch die Kombination unterschiedlicher Untersuchungsmethoden lässt sich die Sicherheit erhöhen.

Bei einem Verdacht auf eine Bedrohung emuliert der heuristische Analysator die Ausführung des Objekts in einer ungefährlichen virtuellen Umgebung des Programms. Wenn bei der Ausführung des Objekts verdächtige Aktionen erkannt werden, wird das Objekt als schädlich eingestuft. Der Start des Objekts wird auf dem Computer gesperrt oder der Benutzer wird nach dem weiteren Vorgehen gefragt:

- Bedrohung in die Quarantäne verschieben, um sie später mit Hilfe aktualisierter Datenbanken zu untersuchen und zu verarbeiten.
- Objekt löschen.
- Überspringen, wenn Sie absolut sicher sind, dass das Objekt unschädlich ist.

Um die heuristischen Methoden zu verwenden, aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**. Zusätzlich können Sie die Genauigkeitsstufe der Untersuchung anpassen. Bewegen Sie dazu den Schieberegler auf die gewünschte Position: oberflächlich, mittel oder tief. Durch die Genauigkeitsstufe lässt sich das Verhältnis von Ausführlichkeit und damit Qualität der Suche nach neuen Bedrohungen zu dem Auslastungsniveau der Systemressourcen und der Untersuchungsdauer regulieren. Je höher die Genauigkeitsstufe der heuristischen Analyse, desto mehr Systemressourcen sind für die Untersuchung erforderlich und desto länger dauert der Vorgang.

Achtung!

Die Kaspersky-Lab-Spezialisten analysieren neue Bedrohungen, die mit Hilfe der heuristischen Analyse gefunden werden, umgehend und fügen den im Stundenrhythmus erscheinenden Programm-Datenbanken entsprechende Desinfektionsmethoden zu hinzu.

Wenn Sie die Programm-Datenbanken regelmäßig aktualisieren, wird das optimale Schutzniveau für den Computer gewährleistet.

Hardware- und Softwarevoraussetzungen

Um die normale Funktionsfähigkeit der Anwendung zu gewährleisten, muss der Computer mindestens folgende Voraussetzungen erfüllen:

Allgemeine Voraussetzungen:

- 75 MB freier Speicher auf der Festplatte.
- CD-ROM-Laufwerk (zur Installation der Anwendung von CD-ROM).
- Eingabegerät, z.B. Maus.
- Microsoft Internet Explorer Version 5.5 oder höher (für das Update der Datenbanken und Programm-Module über das Internet).
- Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (Service Pack 2 oder höher), Microsoft Windows XP Professional (Service Pack 2 oder höher), Microsoft Windows XP Professional x64 Edition:

- Prozessor Intel Pentium 300 MHz oder höher (oder ein entsprechender kompatibler Prozessor).
- 256 MB Arbeitsspeicher.

Microsoft Windows Vista Starter x32, Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

- Prozessor Intel Pentium 800 MHz 32-Bit (x86) / 64-Bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor).
- 512 MB Arbeitsspeicher.

BEDROHUNGEN FÜR DIE COMPUTERSICHERHEIT

Einen Großteil der Bedrohungen für die Computersicherheit bilden riskante Programme. Daneben können auch Spam, Phishing, Hackerangriffe und Werbebanner eine Gefahr darstellen. Diese Bedrohungen sind mit der Verwendung des Internets verbunden.

IN DIESEM ABSCHNITT

Bedrohliche Programme 16

Internet-Bedrohungen 37

BEDROHLICHE PROGRAMME

Die Kaspersky-Lab-Anwendung kann auf einem Computer hunderttausende unterschiedliche gefährliche Programme erkennen. Manche schädlichen Programme stellen eine große Gefahr für den Computer des Benutzers dar, andere sind nur unter bestimmten Bedingungen riskant. Wenn die Anwendung ein gefährliches Programm findet, klassifiziert sie es und weist ihm eine Gefahrenstufe (hoch oder mittel) zu.

Die Virenanalytiker von Kaspersky Lab unterscheiden zwei Hauptkategorien: schädliche Programme und potentiell unerwünschte Programme.

Schädliche Programme (s. S. 17) (Malware) werden speziell dazu geschaffen, um Computern und ihren Benutzern Schaden zuzufügen. Sie sollen z.B. Informationen stehlen, blockieren, verändern oder vernichten, und die Funktion von Computern oder Computernetzwerken stören.

Potentiell unerwünschte Programme (s. S. 30) (PUPs – potentially unwanted programs) sind im Gegensatz zu den schädlichen Programmen, nicht speziell dafür vorgesehen, Schaden anzurichten, können aber trotzdem dazu dienen, die Computersicherheit zu stören.

Die Viren-Enzyklopädie (http://www.viruslist.com/de/viruses/encyclopedia) enthält eine ausführliche Beschreibung dieser Programme.

SCHÄDLICHE PROGRAMME

Schädliche Programme werden speziell dazu geschaffen, um Computern und deren Benutzern Schaden zuzufügen: Sie sollen Informationen stehlen, blockieren, verändern oder zerstören, die Funktion von Computern oder Computernetzwerken stören.

Die schädlichen Programme werden in drei Unterkategorien eingeteilt: *Viren* und *Würmer*, *trojanische Programme* und *schädliche Tools*.

Viren und Würmer (s. S. 17) (Viruses_and_Worms) können Kopien von sich anfertigen, die wiederum selbst reproduktionsfähig sind. Einige von ihnen starten sich selbst ohne Zutun des Benutzers, andere erfordern Benutzeraktionen für ihren Start. Diese Programme beginnen, ihre schädlichen Aktionen auszuführen, wenn sie gestartet werden.

Trojanische Programme (s. S. 20) (Trojan_programs) fertigen im Gegensatz zu Würmern und Viren keine Kopien von sich an. Sie dringen z.B. über E-Mails oder über den Webbrowser in den Computer ein, wenn der Benutzer eine "infizierte" Webseite besucht. Für ihren Start sind Aktionen des Benutzers erforderlich. Sie beginnen, ihre schädlichen Aktionen beim Start auszuführen.

Schädliche Tools (s. S. 27) (Malicous_tools) werden speziell dazu geschaffen, um Schaden anzurichten. Im Gegensatz zu anderen Schadprogrammen führen sie nicht gleich beim Start schädliche Aktionen aus, sondern können auf dem Benutzercomputer gespeichert sein und gestartet werden, ohne Schaden zu verursachen. Diese Programme besitzen Funktionen, die zur Herstellung von Viren, Würmern und trojanischen Programmen, zur Organisation von Netzwerkangriffen auf Remote-Server, zum "Einbruch" in Computer oder für andere schädliche Aktionen verwendet werden.

VIREN UND WÜRMER

Unterkategorie: Viren und Würmer (Viruses_and_Worms)

Gefahrenstufe: hoch

Klassische Viren und Würmer führen auf dem Computer Aktionen aus, die nicht vom Benutzer autorisiert sind, und können Kopien von sich anfertigen, die wiederum selbst reproduktionsfähig sind.

Klassischer Virus

Ist ein klassischer Virus in ein System eingedrungen, dann infiziert er eine bestimmte Datei, wird darin aktiviert, führt seine schädliche Aktion aus und fügt seine Kopien danach in andere Dateien ein.

Ein klassischer Virus vermehrt sich nur auf den lokalen Computerressourcen und kann nicht selbständig in andere Computer eindringen. Auf andere Computer

kann er nur gelangen, wenn er seine Kopie in eine Datei einfügt, die in einem gemeinsamen Ordner oder auf einer CD gespeichert wird, oder wenn der Benutzer eine E-Mail verschickt, an die eine infizierte Datei angehängt ist.

Der Code eines klassischen Virus kann in unterschiedliche Bereiche eines Computers, Betriebssystems oder Programms eindringen. Nach dem Milieu werden Dateiviren, Bootviren, Skriptviren und Makroviren unterschieden.

Viren verfügen über unterschiedliche Infektionsmethoden. Überschreibende Viren (Overwriting) schreiben ihren Code an die Stelle des Codes der infizierten Datei und zerstören ihren Inhalt. Die infizierte Datei funktioniert nicht mehr und kann nicht wiederhergestellt werden. Parasitäre Viren (Parasitic) verändern Dateien, wobei diese voll oder teilweise funktionsfähig bleiben. Companion-Viren (Companion) ändern Dateien nicht, sondern legen Zwillingsdateien an. Beim Öffnen der infizierten Datei wird der Zwilling, also der Virus gestartet. Weitere Virentypen sind Linkviren (Link), Viren, die Objektmodule (OBJ), Compiler-Bibliotheken (LIB) oder den Quelltext von Programmen infizieren, u.a.

Würmer

Der Code eines Wurms wird wie der Code klassischer Viren nach dem Eindringen in einen Computer aktiviert und führt seine schädliche Aktion aus. Die Bezeichnung geht aber darauf zurück, dass er wie ein Wurm von Computer zu Computer "kriechen" und ohne Erlaubnis des Benutzers seine Kopien über verschiedene Datenkanäle verbreiten kann.

Das grundlegende Merkmal, nach dem Würmer voneinander unterschieden werden, ist die Art der Weiterverbreitung. Die folgende Tabelle bietet eine Beschreibung der Wurmtypen unterschieden nach der Ausbreitungsmethode.

Tabelle 1. Würmer nach der Art ihrer Ausbreitung

TYP	BEZEICHNUNG	BESCHREIBUNG
Email-Worm	Mailwürmer	Sie verbreiten sich über E-Mails. Eine infizierte E-Mail enthält eine angehängte Datei mit der Kopie eines Wurms oder einen Link zu dieser Datei auf einer übernommenen Webseite oder Hackerseite. Wenn Sie die angehängte Datei öffnen, wird der Wurm aktiviert. Wenn Sie auf den Link klicken, wird die Datei heruntergeladen und anschließend geöffnet, und der Wurm beginnt ebenfalls, seine schädlichen Aktionen auszuführen. Danach fährt er fort, seine Kopien weiterzuverbreiten. Dazu sucht er andere E-Mail-Adressen und verschickt infizierte Nachrichten an sie.

Typ	**Bezeichnung**	**Beschreibung**
IM-Worm	Würmer für Instant-Messenger	Sie breiten sich über Instant-Messenger (Systeme zum direkten Nachrichtenaustausch) wie beispielsweise ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager und Skype aus. Gewöhnlich verschickt ein IM-Wurm an die Adressen aus Kontaktlisten Nachrichten, die einen Link zu einer Datei mit seiner Kopie auf einer Webseite enthalten. Wenn der Benutzer die Datei herunterlädt und öffnet, wird der Wurm aktiviert.
IRC-Worm	Würmer für Internet-Chats	Sie verbreiten sich über Internet Relay Chats, d.h. Dienstsysteme, mit deren Hilfe man über das Internet in Echtzeit mit anderen Benutzern kommunizieren kann. Der Wurm publiziert im Internet-Chat eine Datei mit seiner Kopie oder einen Link zu einer Datei. Wenn der Benutzer die Datei herunterlädt und öffnet, wird der Wurm aktiviert.
Net-Worm	Netzwerkwürmer (Würmer für Computernetz-werke)	Sie verbreiten sich über Computernetzwerke. Im Gegensatz zu anderen Wurmtypen verbreiten sich Netzwerkwürmer ohne das Zutun eines Benutzers aus. Der Wurm sucht im lokalen Netzwerk nach Computern, auf denen Programme verwendet werden, die Schwachstellen aufweisen. Zu diesem Zweck verschickt er ein speziell erstelltes Netzwerkpaket (Exploit), das den Wurmcode oder einen Ausschnitt davon enthält. Befindet sich ein "verwundbarer" Computer im Netzwerk, dann empfängt dieser das Netzwerkpaket. Nachdem der Wurm vollständig in den Computer eingedrungen ist, wird er aktiviert.

TYP	BEZEICHNUNG	BESCHREIBUNG
P2P-Worm	Würmer für Dateitausch-netzwerke	Sie werden über Dateitausch-Peering-Netzwerke wie Kazaa, Grokster, EDonkey, FastTrack und Gnutella verbreitet. Um in das Netzwerk einer Dateitauschbörse einzudringen, kopiert sich der Wurm in einen Ordner für den Dateitausch, der sich normalerweise auf einem Benutzercomputer befindet. Das Dateitauschnetzwerk zeigt Informationen über diese Datei an und ein Benutzer kann die infizierte Datei im Netzwerk "finden", herunterladen und öffnen. Kompliziertere Würmer imitieren das Netzwerkprotokoll eines konkreten Dateitauschnetzwerks: Sie geben positive Antworten auf Suchanfragen und bieten ihre Kopien zum Download an.
Worm	Sonstige Würmer	Zu den sonstigen Netzwerkwürmern gehören: • Würmer, die ihre Kopien über Netzwerkressourcen verbreiten. Unter Verwendung von Funktionen des Betriebssystems durchsuchen sie verfügbare Netzwerkordner, bauen nach dem Zufallsprinzip Verbindungen mit Computern im globalen Netzwerk auf, und versuchen, vollständigen Zugriff auf deren Laufwerke zu erhalten. Im Gegensatz zu Würmern für Computernetzwerke muss der Benutzer die Datei mit der Kopie des Wurms öffnen, um ihn zu aktivieren. • Würmer, die sich durch andere Methoden ausbreiten, wie in dieser Tabelle beschrieben (z.B. Ausbreitung über Mobiltelefone).

TROJANISCHE PROGRAMME

Unterkategorie: Trojanische Programme (Trojan_programs)

Gefahrenstufe: hoch

Im Gegensatz zu Würmern und Viren erstellen trojanische Programme keine Kopien von sich. Sie dringen z.B. über E-Mails oder über den Webbrowser in den Computer ein, wenn der Benutzer eine "infizierte" Webseite besucht. Trojanische Programme werden unter Beteiligung des Benutzers gestartet. Sie beginnen, ihre schädliche Aktion beim Start auszuführen.

Die einzelnen Gruppen von trojanischen Programmen verhalten sich unterschiedlich auf einem infizierten Computer. Die Hauptfunktionen von Trojanern sind das Sperren, Verändern oder Vernichten von Informationen, sowie die Störung der Funktionen von Computern oder Computernetzwerken. Außerdem können trojanische Programme Dateien empfangen oder senden, Dateien ausführen, auf dem Bildschirm Meldungen anzeigen, auf Webseiten zugreifen, Programme herunterladen und installieren, und den Computer neu starten.

Häufig verwenden Angreifer eine "Kombination" aus unterschiedlichen trojanischen Programmen.

Die folgende Tabelle beschreibt die Typen der trojanischen Programme nach ihrem Verhalten.

Tabelle 2. Typen der trojanischen Programme nach ihrem Verhalten auf dem infizierten Computer

TYP	**BEZEICHNUNG**	**BESCHREIBUNG**
Trojan-ArcBomb	Trojanische Programme - "Archivbomben"	Archive. Beim Extrahieren vergrößert sich der Inhalt so stark, dass die Arbeit des Computers gestört wird. Sobald versucht wird, ein solches Archiv zu entpacken, kann sich die Arbeit des Computers verlangsamen oder er bleibt hängen, und die Festplatte kann mit einer großen Menge "leerer" Daten gefüllt werden. Eine besondere Gefahr bilden "Archivbomben" für Datei- und Mailserver. Wenn auf dem Server ein System zur automatischen Verarbeitung eingehender Daten verwendet wird, kann eine "Archivbombe" den Server zum Absturz bringen.
Backdoor	Trojanische Programme zur Remote-Administration	Dieser Typ gilt unter den trojanischen Programmen als der gefährlichste. Ihrer Funktion nach gleichen sie legalen Programmen zur Remote-Administration. Diese Programme installieren sich ohne Wissen des Benutzers auf dem Computer und erlauben dem Angreifer die Fernsteuerung des Computers.

TYP	BEZEICHNUNG	BESCHREIBUNG
Trojan	Trojanische Programme	Dieser Typ umfasst folgende Schadprogramme: • **klassische trojanische Programme**. Sie führen nur die Grundfunktionen trojanischer Programme aus: Sperrung, Veränderung oder Zerstörung von Informationen, Störung der Arbeit von Computern oder Computernetzwerken. Sie besitzen keine Zusatzfunktionen, über die andere Typen trojanischer Programme verfügen, die in dieser Tabelle beschrieben sind. • **"Mehrzweck"-Trojaner**. Sie besitzen Zusatzfunktionen, die gleichzeitig für mehrere Typen trojanischer Programme charakteristisch sind.
Trojan-Ransom	Trojanische Erpressungs-programme	Sie nehmen die Informationen auf dem Computer als "Geisel", verändern oder sperren sie, oder stören die Arbeit des Computers, damit der Benutzer nicht mehr auf seine Informationen zugreifen kann. Der Angreifer fordert vom Benutzer ein "Lösegeld" und verspricht, dafür ein Programm zu liefern, das die Funktionsfähigkeit des Computers und der Daten wiederherstellt.
Trojan-Clicker	Trojanische Clicker-Programme	Trojan-Clicker greifen von einem Benutzercomputer aus auf Webseiten zu: Sie senden entweder selbst Befehle an den Webbrowser oder ersetzen Webadressen, die in Systemdateien gespeichert sind. Mit Hilfe dieser Programme organisieren Angreifer Netzwerkangriffe oder steigern die Besucherzahl von Seiten, um die Anzeigehäufigkeit von Werbebannern zu erhöhen.

TYP	**BEZEICHNUNG**	**BESCHREIBUNG**
Trojan-Downloader	Trojanische Download-Programme	Sie greifen auf eine Webseite des Angreifers zu, laden von dort andere Schadprogramme herunter und installieren sie auf dem Benutzercomputer. Sie können den Dateinamen der herunterzuladenden Malware in sich speichern oder ihn von der Webseite erhalten, auf die sie zugreifen.
Trojan-Dropper	Trojanische Installations-programme	Nachdem sie auf der Computerfestplatte gespeichert wurden, installieren sie andere trojanische Programme, die sich in ihrem Körper befinden. Angreifer können trojanische Installationsprogramme verwenden: • um ohne Wissen des Benutzers ein schädliches Programm zu installieren: Der "Installationstrojaner" zeigt keinerlei Meldungen an oder blendet falsche Meldungen über einen Fehler im Archiv oder eine inkorrekte Version des Betriebssystems ein; • um andere bekannte Malware vor der Entdeckung zu schützen: Nicht alle Antiviren-Programme können Malware in trojanischen Installationsprogrammen erkennen.

Typ	**Bezeichnung**	**Beschreibung**
Trojan-Notifier	Trojanische Benachrichtigungs-programme	Sie informieren den Angreifer darüber, dass der infizierte Computer "verfügbar" ist und übermitteln folgende Informationen über den Computer: IP-Adresse des Computers, Nummer des offenen Ports, E-Mail-Adresse. Sie nehmen per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise Kontakt mit dem Angreifer auf. Dieser Typ der Trojaner wird häufig in Kombinationen aus unterschiedlichen trojanischen Programmen verwendet. Sie teilen dem Angreifer mit, dass andere trojanische Programme erfolgreich auf dem Computer installiert wurden.
Trojan-Proxy	Trojanische Proxy-Programme	Sie ermöglichen es dem Angreifer, über den Computer des Benutzers anonym auf Webseiten zuzugreifen. Häufig dienen sie zur Spam-Versendung.
Trojan-PSW	Trojanische Programme zum Kennwortdiebstahl	Trojanische Programme, die Kennwörter stehlen (Password Stealing Ware). Sie berauben Benutzerkonten und stehlen beispielsweise Registrierungsdaten für Softwareprodukte. Sie durchsuchen Systemdateien und Systemregistrierung nach vertraulichen Informationen und schicken diese per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer. Einige dieser trojanischen Programme gehören speziellen Typen an, die in dieser Tabelle beschrieben sind. Dazu zählen Trojaner, die Bankkonten berauben (Trojan-Banker), Daten von Internet-Messengern stehlen (Trojan-IM) und Daten aus Netzwerkspielen entwenden (Trojan-GameThief).

TYP	**BEZEICHNUNG**	**BESCHREIBUNG**
Trojan-Spy	Trojanische Spyware-Programme	Diese Trojaner spionieren den Benutzer auf elektronische Weise aus: Sie sammeln Informationen über seine Aktionen auf dem Computer, fangen z.B. über die Tastatur eingegebene Informationen ab, machen Screenshots und legen eine Liste der aktiven Programme an. Die gesammelten Informationen werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-DDoS	Trojanische Programme für Netzwerkangriffe	Sie schicken eine große Anzahl von Anfragen vom Benutzercomputer an einen Remote-Server. Das bringt den Server zum Absturz, weil seine Ressourcen nicht ausreichen, um die eingehenden Anfragen zu verarbeiten (DoS = Denial of Service, Dienstverweigerung). Häufig werden viele Computer von solchen Programmen infiziert, um sie danach gleichzeitig für einen Angriff auf einen Server zu verwenden.
Trojan-IM	Trojanische Programme zum Diebstahl der Daten von Internet-Messenger-Benutzern	Sie stehlen Nummern und Kennwörter der Benutzer von Internet-Messengern (Systeme zum direkten Nachrichtenaustausch) wie ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager oder Skype. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.

TYP	BEZEICHNUNG	BESCHREIBUNG
Rootkit	Rootkits	Sie tarnen andere Malware und deren Aktivität, damit sich diese möglichst lang im infizierten System verbergen können. Rootkits können Dateien, Prozesse im Arbeitsspeicher des infizierten Computers oder Registrierungsschlüssel, die Schadprogramme starten, maskieren. Außerdem können sie den Datenaustausch zwischen Programmen auf dem Benutzercomputer und auf anderen Netzwerkcomputern verheimlichen.
Trojan-SMS	Trojanische Programme für SMS-Nachrichten	Sie infizieren Handys und schicken von diesen SMS-Nachrichten an kostenpflichtige Nummern.
Trojan-GameThief	Trojanische Programme zum Diebstahl von Daten der Benutzer von Netzwerkspielen	Sie stehlen Daten von Benutzerkonten, die an Computernetzwerkspielen teilnehmen. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-Banker	Trojanische Programme zum Diebstahl von Daten über Bankkonten	Sie stehlen Daten von Benutzerkonten, die an Computernetzwerkspielen teilnehmen. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-Mailfinder	Trojanische Programme zum Sammeln von E-Mail-Adressen	Sie sammeln auf dem Computer E-Mail-Adressen und übermitteln diese per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer. An die gesammelten Adressen kann der Angreifer Spam verschicken.

Schädliche Tools

Unterkategorie: Schädliche Tools (Malicious_tools)

Gefahrenstufe: mittel

Schädliche Tools werden speziell dazu geschaffen, um Schaden anzurichten. Im Gegensatz zu anderen Schadprogrammen führen sie nicht gleich beim Start schädliche Aktionen aus, sondern können auf dem Benutzercomputer gespeichert sein und gestartet werden, ohne Schaden zu verursachen. Diese Programme besitzen Funktionen, die zur Herstellung von Viren, Würmern und trojanischen Programmen, zur Organisation von Netzwerkangriffen auf Remote-Server, zum "Einbruch" in Computer oder für andere schädliche Aktionen verwendet werden.

Die schädlichen Tools werden im Hinblick auf ihre Funktionen unterschieden. Die Typen werden in folgender Tabelle beschrieben.

Tabelle 3. Schädliche Tools nach ihren Funktionen

Typ	Bezeichnung	Beschreibung
Constructor	Konstrukteure	Mit ihrer Hilfe können neue Viren, Würmer und trojanische Programme hergestellt werden. Einige Konstrukteure besitzen eine standardmäßige Fensteroberfläche, in dem über ein Menü der Typ des Schadprogramms, die Tarnmethode gegen Debugger und andere Eigenschaften gewählt werden können.
Dos	Netzwerkangriffe	Sie schicken eine große Anzahl von Anfragen vom Benutzercomputer an einen Remote-Server. Das bringt den Server zum Absturz, weil seine Ressourcen nicht ausreichen, um die eingehenden Anfragen zu verarbeiten (DoS = Denial of Service, Dienstverweigerung).

TYP	BEZEICHNUNG	BESCHREIBUNG
Exploit	Exploits	Exploits stellen eine Datenkombination oder einen Programmcode dar, der die Schwachstellen des Programms, in dem er verarbeitet wird, ausnutzt, um auf dem Computer eine schädliche Aktion auszuführen. Ein Exploit kann beispielsweise Dateien schreiben oder lesen, oder auf "infizierte" Webseiten zugreifen. Bestimmte Exploits verwenden Schwachstellen unterschiedlicher Programme oder Netzwerkdienste. Exploits werden in Form eines Netzwerkpakets über ein Netzwerk auf viele Computer übertragen, um Computer mit verletzbaren Netzwerkdiensten zu finden. Ein Exploit in einer DOC-Datei verwendet die Schwachstellen eines Textverarbeitungsprogramms. Er kann damit beginnen, die vom Angreifer programmierten Funktionen auszuführen, wenn der Benutzer die infizierte Datei öffnet. Ein Exploit, der in eine E-Mail eingebettet wurde, sucht nach Schwachstellen in einem E-Mail-Programm. Er kann mit der Ausführung einer schädlichen Aktion beginnen, sobald der Benutzer die infizierte E-Mail in einem bestimmten Programm öffnet. Mit Hilfe von Exploits werden Netzwürmer (Net-Worm) verbreitet. Exploits des Typs Nuker (Nuker) (Nuker) bestehen aus Netzwerkpaketen, die einen Computer zum Absturz bringen.
FileCryptor	Chiffreure	Chiffreure verschlüsseln andere Malware, um sie vor einem Antiviren-Programm zu verstecken.

TYP	BEZEICHNUNG	BESCHREIBUNG
Flooder	Programme zur "Verunreinigung" von Netzwerken	Sie verschicken eine große Anzahl von Nachrichten über Netzwerkkanäle. Zu dieser Klasse zählen beispielsweise Programme, die der "Verunreinigung" von Internet Relay Chats dienen. Programme, die der "Verunreinigung" von Kanälen für E-Mail, Instant-Messenger und Mobilfunksysteme dienen, gehören nicht zu dieser Gruppe. Diese Programme werden separaten Typen zugeordnet, die ebenfalls in dieser Tabelle beschrieben sind (Email-Flooder, IM-Flooder und SMS-Flooder).
HackTool	Hacker-Tools	Hacker-Tools können die Kontrolle über den Computer, auf dem sie installiert sind, übernehmen oder einen anderen Computerangreifen (z.B. ohne Erlaubnis des Benutzers andere Systembenutzer hinzufügen und Systemberichte löschen, um ihre Spuren im System zu verwischen). Zu ihnen gehören bestimmte Sniffer, die über schädlichen Funktionen wie z.B. das Abfangen von Kennwörtern verfügen. Sniffer sind Programme, die den Netzwerkverkehr abhören können.
not-virus:Hoax	Böse Scherze	Diese Programme erschrecken den Benutzer mit virenähnlichen Meldungen: Sie zeigen fiktive Meldungen über Virenfunde in sauberen Dateien oder über das Formatieren der Festplatte an.
Spoofer	Imitator-Tools	Sie schicken E-Mails und Netzwerkanfragen mit gefälschten Absenderadressen. Angreifer verwenden Imitatoren beispielsweise, um sich als Absender auszugeben.
VirTool	Tools zur Modifikation schädlicher Programme	Sie erlauben es, andere Malware so zu modifizieren, dass sie sich vor Antiviren-Programmen verstecken können.

TYP	BEZEICHNUNG	BESCHREIBUNG
Email-Flooder	Programme zur "Verunreinigung" von Mailboxen	Sie schicken eine große Anzahl von Nachrichten an E-Mail-Adressen ("verstopfen sie mit Müll"). Die große Menge von Briefen hindert den Benutzer daran, nützliche Post zu erkennen.
IM-Flooder	Programme zur "Verunreinigung" von Instant-Messengern	Sie senden eine große Anzahl von Nachrichten an die Benutzer von Instant-Messengern (Systemen zum direkten Nachrichtenaustausch) wie ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager oder Skype. Die große Menge von Nachrichten hindert den Benutzer daran, nützliche Post zu erkennen.
SMS-Flooder	Programme zur "Verunreinigung" mit SMS-Nachrichten	Sie schicken eine große Anzahl von SMS-Nachrichten an Handys.

POTENTIELL UNERWÜNSCHTE PROGRAMME

Potentiell unerwünschte Programme sind im Gegensatz zu den schädlichen Programmen, nicht speziell dafür vorgesehen, Schaden anzurichten. Trotzdem kann mit ihrer Hilfe die Computersicherheit bedroht werden.

Zu den potentiell unerwünschten Programmen zählen *Adware, Programme mit pornografischem Charakter* und *sonstige potentiell unerwünschte Programme*.

Adware-Programme (s. S. 31) (Adware) dienen dazu, dem Benutzer Werbeinformationen zu zeigen.

Programme mit pornografischem Charakter (s. S. 31) (Porwnware) dienen dazu, dem Benutzer Informationen mit pornografischem Inhalt zu zeigen.

Die sonstigen potentiell unerwünschten Programme (s. S. 32) (Riskware) sind überwiegend nützliche Programme, die von vielen Anwendern benutzt werden. Wenn allerdings ein Angreifer Zugriff auf diese Programme erhält oder sie im Computer des Benutzers installiert, können ihre Funktionen dazu dienen, die Sicherheit zu verletzen.

Für die Installation von potentiell unerwünschten Programmen gibt es die beiden folgenden Varianten:

- Der Benutzer installiert die Programme einzeln oder zusammen mit einem anderen Programm (Beispielsweise integrieren manche Hersteller Adware-Programme in kostenlose oder bedingt kostenlose Software).
- Sie werden von Angreifern installiert. Dazu werden sie beispielsweise in Pakete mit anderer Malware integriert, oder es werden Webbrowser-Schwachstellen oder trojanische Download- und Installationsprogramme verwendet.

ADWARE

Unterkategorie: Programme mit Werbecharakter (Adware)

Gefahrenstufe: mittel

Adware-Programme dienen dazu, dem Benutzer Werbeinformationen zu zeigen. Sie zeigen Werbebanner auf der Oberfläche anderer Programme an oder leiten Suchanfragen auf Webseiten mit Werbung um. Einige von ihnen sammeln auf Werbung bezogene Informationen über den Benutzer und leiten sie an ihren Urheber weiter, z.B. Informationen darüber, welche Seiten der Benutzer besucht und welche Suchanfragen er vornimmt (im Gegensatz zu trojanischer Spyware leiten sie diese Informationen mit der Erlaubnis des Benutzers weiter.)

PROGRAMME MIT PORNOGRAFISCHEM CHARAKTER

Unterkategorie: Programme mit pornografischem Charakter (Pornware)

Gefahrenstufe: mittel

Gewöhnlich installieren Benutzer solche Programme selbst, um pornografische Informationen zu suchen und herunterzuladen.

Solche Programme werden auch von Angreifern auf dem Computer eines Benutzers installiert, um ohne dessen Erlaubnis Werbung von kostenpflichtigen pornografischen Seiten und Diensten zu präsentieren. Zur Installation verwenden sie Schwachstellen des Betriebssystems oder des Webbrowsers, trojanische Download-Programme und trojanische Installationsprogramme.

Nach ihren Funktionen werden drei Typen von Pornware-Programmen unterschieden. Die Typen werden in folgender Tabelle beschrieben.

Tabelle 4. Typen der Programme mit pornografischem Charakter nach ihren Funktionen

TYP	BEZEICHNUNG	BESCHREIBUNG
Porn-Dialer	Automatische Einwahl-programme	Sie rufen pornografische Telefondienste an (deren Telefonnummern sie gespeichert haben). Im Gegensatz zu trojanischen Dialern benachrichtigen sie den Benutzer von ihren Aktionen.
Porn-Downloader	Programme zum Download von Dateien aus dem Internet	Sie laden Daten mit pornografischem Inhalt auf den Computer herunter. Im Gegensatz zu trojanischen Dialern benachrichtigen sie den Benutzer von ihren Aktionen.
Porn-Tool	Tools	Sie erlauben die Suche und Anzeige pornografischer Materialien. Zu ihnen gehören spezielle Symbolleisten für Browser oder spezifische Video Player.

SONSTIGE POTENTIELL UNERWÜNSCHTE PROGRAMME

Unterkategorie: sonstige potentiell unerwünschte Programme (Riskware)

Gefahrenstufe: mittel

Die Mehrzahl dieser Programme sind nützliche Programme. Sie werden von vielen Anwendern benutzt. Als Riskware zählen IRC-Clients, Dialer, Programme für den Datei-Download, Aktivitätsmonitore für Computersysteme, Tools für die Arbeit mit Kennwörtern sowie Internetserver für die Dienste FTP, HTTP oder Telnet.

Wenn allerdings ein Angreifer Zugriff auf diese Programme erhält oder sie im Computer des Benutzers installiert, können bestimmte Funktionen dazu dienen, die Sicherheit zu verletzen.

Sonstige potentiell unerwünschte Programme werden nach ihren Funktionen unterschieden. Die Typen werden in folgender Tabelle beschrieben.

Tabelle 5. Typen der sonstigen potentiell unerwünschten Programme nach ihren Funktionen

TYP	**BEZEICHNUNG**	**BESCHREIBUNG**
Client-IRC	Clients für Internet-Chats	Diese Programme werden von Benutzern installiert, um in Internet Relay Chats zu kommunizieren. Angreifer verwenden sie zur Verbreitung schädlicher Programme.
Dialer	Automatische Einwahlprogramme	Dialer können heimlich Telefonverbindungen über ein Modem herstellen.
Downloader	Download-Programme	Downloader können heimlich Dateien von Webseiten herunterladen.
Monitor	Monitorprogramme	Monitore können die Aktivitäten auf dem Computer, auf dem sie installiert sind, beobachten (Sie überwachen, welche Programme laufen und wie sie Daten mit Programmen auf anderen Computern austauschen).
PSWTool	Programme zur Wiederherstellung von Kennwörtern	Sie erlauben es, vergessene Kennwörter zu lesen und wiederherzustellen. Zu diesem Zweck werden sie auch heimlich von Angreifern auf Benutzercomputern installiert.

TYP	BEZEICHNUNG	BESCHREIBUNG
RemoteAdmin	Programme zur Remote-Administration	RemoteAdmins werden häufig von Systemadministratoren verwendet. Sie bieten Zugriff auf die Oberfläche eines Remote-Computers, der dadurch überwacht und gesteuert werden kann. Zu diesem Zweck werden sie auch heimlich von Angreifern auf Benutzercomputern installiert, um Remote-Computer zu beobachten und zu steuern. Potentiell unerwünschte Programme zur Remote-Administration unterscheiden sich von trojanischen Fernsteuerungsprogrammen des Typs Backdoor. Trojanische Programme besitzen Funktionen, die ihnen erlauben, selbständig in ein System einzudringen und sich zu installieren. Potentiell unerwünschte Programme verfügen nicht über diese Funktionen.
Server-FTP	FTP-Server	Sie erfüllen die Funktionen eines FTP-Servers. Angreifer installieren sie auf dem Benutzercomputer, um Remote-Zugriff über das FTP-Protokoll zu erhalten.
Server-Proxy	Proxyserver	Sie erfüllen die Funktionen eines Proxyservers. Angreifer installieren sie auf dem Benutzercomputer, um in seinem Namen Spam zu verschicken.
Server-Telnet	Telnet-Server	Sie erfüllen die Funktionen eines Telnet-Servers. Angreifer installieren sie auf dem Benutzercomputer, um Remote-Zugriff über das Telnet-Protokoll zu erhalten.

TYP	**BEZEICHNUNG**	**BESCHREIBUNG**
Server-Web	Webserver	Sie erfüllen die Funktionen eines Webservers. Angreifer installieren sie auf dem Benutzercomputer, um Remote-Zugriff über das HTTP-Protokoll zu erhalten.
RiskTool	Tools für die Arbeit auf dem lokalen Computer	Sie bieten dem Benutzer bei der Arbeit auf seinem Computer zusätzliche Möglichkeiten (Dateien oder aktive Programmfenster auf dem Computer verstecken, aktive Prozesse beenden).
NetTool	Netzwerk-Tools	Sie bieten dem Benutzer des Computers, auf dem sie installiert sind, zusätzliche Möglichkeiten bei der Arbeit mit anderen Computern in einem Netzwerk (andere Computer neu starten, offene Ports suchen, Programme starten, die auf einem anderen Computer installiert sind).
Client-P2P	Clients für Peering-Netzwerke	Sie erlauben die Arbeit in Peering-Netzwerken (Peer-to-Peer). Angreifer können sie zur Verbreitung schädlicher Programme verwenden.
Client-SMTP	SMTP-Clients	SMTP-Clients verschicken um Hintergrund E-Mails. Angreifer installieren sie auf dem Benutzercomputer, um in seinem Namen Spam zu verschicken.
WebToolbar	Web-Symbolleisten	Sie fügen Symbolleisten für die Verwendung von Suchmaschinen in die Oberfläche anderer Programme ein.

TYP	BEZEICHNUNG	BESCHREIBUNG
FraudTool	Pseudoprogramme	Sie geben sich als andere Programme aus . Es gibt beispielsweise Pseudo-Antiviren-Programme, die Meldungen über den Fund schädlicher Programme ausgeben, in Wirklichkeit aber keine Funktionen zur Virensuche oder Desinfektion besitzen.

WIE DIE ANWENDUNG INFIZIERTE, VERDÄCHTIGE UND POTENTIELL GEFÄHRLICHE OBJEKTE ERKENNT

Die Kaspersky-Lab-Anwendung verwendet zwei Methoden, um schädliche Programme in Objekten zu erkennen: reaktive (unter Verwendung von Datenbanken) und proaktive (unter Verwendung der heuristischen Analyse).

Die Datenbanken bestehen aus Dateien mit Einträgen, die es erlauben, in untersuchten Objekten hunderttausende von bekannten Schadprogrammen zu identifizieren. Diese Einträge enthalten Informationen über Kontrollabschnitte des Malware-Codes und Algorithmen zur Desinfektion von Objekten, in denen diese Programme gefunden werden. Die Virenanalytiker von Kaspersky Lab finden täglich mehrere hundert neue Schadprogramme, erstellen Einträge zu deren Identifikation und nehmen diese in die Datenbank-Updates auf.

Findet die Kaspersky-Lab-Anwendung in einem Untersuchungsobjekt Codeabschnitte, die vollständig mit den in der Datenbank verzeichneten Kontrollabschnitten für den Code eines bestimmten Schädlings übereinstimmen, dann wird das Objekt als infiziert betrachtet. Bei teilweiser Übereinstimmung gilt das Objekt (bei der Erfüllung bestimmter Bedingungen) als verdächtig.

Mit Hilfe der proaktiven Methode ist es möglich, auch die neuesten Schadprogramme zu erkennen, über die noch keine Informationen in den Datenbanken vorhanden sind.

Objekte, die neue Malware enthalten, werden von der Kaspersky-Lab-Anwendung aufgrund ihres Verhaltens entlarvt. Der Code eines solchen Objekts stimmt zwar nicht teilweise oder vollständig mit dem Code eines bekannten Schädlings überein, doch enthält er Befehlsfolgen, die für schädliche Programme typisch sind. Dazu gehören das Öffnen einer Datei, das Schreiben in eine Datei und das Abfangen von Interrupt-Vektoren. Die Anwendung erkennt

beispielsweise, wenn eine Datei aussieht, als sei sie von einem unbekannten Virus infiziert.

Die mit der proaktiven Methode gefundenen Objekte gelten als potentiell gefährlich.

INTERNET-BEDROHUNGEN

Die Kaspersky-Lab-Anwendung verfügt über spezielle Technologien, um den Computer vor folgenden Bedrohungen zu schützen:

- Spam oder unerwünschte eingehende E-Mail (s. Abschnitt "Spam oder unerwünschte eingehende E-Mail" s. S. 37)
- Phishing (s. S. 38)
- Hackerangriffe (s. S. 38)
- Anzeige von Bannern (s. S. 39)

SPAM ODER UNERWÜNSCHTE EINGEHENDE E-MAIL

Die Kaspersky-Lab-Anwendung schützt den Benutzer vor Spam. Als Spam werden unerwünschte eingehende E-Mails bezeichnet, die häufig Werbung enthalten. Spam belastet Datenkanäle und die E-Mail-Server des Providers. Der Empfänger muss für den durch Spam verursachten Datenverkehr bezahlen und der Empfang der normalen E-Mails wird verlangsamt. In vielen Ländern gilt der Spam-Versand deshalb als gesetzwidrig.

Die Kaspersky-Lab-Anwendung untersucht eingehende E-Mails in den Programmen Microsoft Office Outlook, Microsoft Outlook Express und The Bat!. Wird eine Nachricht als Spam erkannt, dann werden die von Ihnen festgelegten Aktionen ausgeführt. Eine Spam-Mail kann z.B. in einen speziellen Ordner verschoben oder gelöscht werden.

Spam wird von der Kaspersky-Lab-Anwendung mit hoher Präzision erkannt. Zur Spam-Filterung werden gleichzeitig mehrere Technologien eingesetzt: Die Absenderadresse sowie Wörter und Phrasen in der Betreffzeile der Nachricht werden analysiert. Spam wird auch in Form von Bildern erkannt und ein lernfähiger Algorithmus zur Spam-Erkennung im Nachrichtentext wird verwendet.

Die Anti-Spam-Datenbanken umfassen "schwarze" und "weiße" Listen für Absenderadressen sowie Listen für Wörter und Phrasen, die unterschiedlichen

Spam-Kategorien wie Werbung, Medizin und Gesundheit, Glücksspiele, u.a. angehören.

PHISHING

Phishing ist eine Art des Internetbetrugs, die im "Angeln" von Kreditkartennummern, PIN-Codes und anderen persönlichen Benutzerdaten besteht. Die Daten werden anschließend zum Diebstahl von Geld verwendet.

Phishing ist häufig mit Internet-Banking verbunden. Der Angreifer erstellt eine genaue Kopie der Webseite einer Bank und schickt unter dem Namen der Bank E-Mails an die Kunden. Sie benachrichtigen darüber, dass aufgrund einer Störung oder des Austausch der Software im Internet-Banking-System die Daten des Benutzerkontos verloren gegangen seien. Deshalb soll der Kunde seine Daten auf der Seite der Bank bestätigen oder ändern. Der Benutzer kann auf einen Link klicken, der zur vom Angreifer gefälschten Webseite führt, und dort seine Daten eingeben.

Die Anti-Phishing-Datenbanken enthalten eine Liste der URL-Adressen von Webseiten, von denen bekannt ist, dass sie für Phishing-Angriffe verwendet werden.

Die Kaspersky-Lab-Anwendung untersucht eingehende E-Mails in den Programmen Microsoft Office Outlook und Microsoft Outlook Express. Wird in einer Nachricht ein Link zu einer URL-Adresse gefunden, die in den Datenbanken vorhanden ist, dann wird die E-Mail als Spam markiert. Wenn der Benutzer die Nachricht öffnet und versucht, dem Link zu folgen, wird die Seite von der Anwendung gesperrt.

HACKERANGRIFFE

Ein *Hackerangriff* besteht im Eindringen in das System eines Remote-Computers, um die Kontrolle darüber zu übernehmen, ihn zum Absturz zu bringen oder Zugriff auf geschützte Informationen zu erhalten.

Als Hackerangriffe bezeichnet man sowohl die Aktionen von Angreifern (z.B. Scannen von Ports, Knacken von Kennwörtern) als auch schädliche Programme, die im Namen des Benutzers Befehle ausführen, ihrem "Herrn" Informationen übermitteln oder andere Funktionen von Hackerangriffen ausführen. Zu ihnen zählen auch bestimmte trojanische Programme, DoS-Angriffe, schädliche Skripts und verschiedene Netzwerkwürmer.

Hackerangriffe breiten sich in lokalen oder globalen Netzwerken über Schwachstellen in Betriebssystemen und Programmen aus. Sie werden bei Verbindungen mit einem Netzwerk als separate IP-Pakete übertragen.

Die Kaspersky-Lab-Anwendung wehrt Hackerangriffe ab, ohne die Netzwerkverbindungen zu stören. Sie verwendet spezielle Firewall-Datenbanken. Diese Datenbanken enthalten Einträge, mit denen IP-Datenpakete identifiziert werden können, die für bestimmte Hackerangriffe charakteristisch sind. Die Kaspersky-Lab-Anwendung analysiert Netzwerkverbindungen und blockiert darin IP-Pakete, die als gefährlich gelten.

Anzeige von Bannern

Banner oder Werbeanzeigen, die einen Link zur Webseite einer werbenden Firma enthalten, besitzen meistens die Form von Bildern. Ihre Anzeige bedroht die Computersicherheit nicht, gilt aber als Störung der normalen Arbeit auf dem Computer. Das Blinken von Bannern auf dem Bildschirm beeinträchtigt die Arbeitsbedingungen und senkt die Leistungsfähigkeit. Der Benutzer wird durch irrelevante Informationen abgelenkt. Durch das Klicken auf Banner wird der Internet-Datenverkehr erhöht.

In vielen Unternehmen bildet das Sperren von Bannern im Interface einen Aspekt der Sicherheitsrichtlinie.

Die Kaspersky-Lab-Anwendung blockiert Banner nach den URL-Adressen der Webseiten, auf die die Banner verweisen. Sie verwendet aktualisierbare Anti-Banner-Datenbanken, die eine Liste von URL-Adressen russischer und internationaler Banner-Netzwerke enthalten. Die Anwendung prüft die Links auf einer Webseite, die heruntergeladen wird, und vergleicht die darin enthaltenen Adressen mit den Datenbanken. Wird eine Übereinstimmung gefunden, dann wird der Link zu dieser Adresse aus der Seite gelöscht und die Seite wird weitergeladen.

INSTALLATION DER ANWENDUNG AUF EINEM COMPUTER

Die Anwendung wird im interaktiven Modus mit Hilfe eines Installationsassistenten auf dem Computer installiert.

Achtung!

Es wird empfohlen, alle laufenden Anwendungen zu beenden, bevor mit der Installation begonnen wird.

Um die Anwendung auf Ihrem Computer zu installieren, starten Sie die Distributionsdatei (Datei mit der Endung *.exe) von der Produkt-CD.

Hinweis

Die Installation der Anwendung von einer Distribution, die aus dem Internet heruntergeladen wurde, ist mit der Installation der Anwendung von einer Distributions-CD vollkommen identisch.

Daraufhin erfolgt die Suche nach dem Installationspaket für die Anwendung (Datei mit der Endung *.msi). Wenn das Paket vorhanden ist, wird geprüft, ob auf den Kaspersky-Lab-Servern im Internet eine neuere Version vorhanden ist. Wird die Datei mit dem Installationspaket nicht gefunden, dann wird Ihnen angeboten, sie herunterzuladen. Nach dem Download wird die Programminstallation gestartet. Bei Ablehnung des Downloads wird die Programminstallation im normalen Modus fortgesetzt.

Das Installationsprogramm besitzt die Form eines Assistenten. Jedes Fenster enthält eine Auswahl von Schaltflächen zur Steuerung des Installationsprozesses. Im Folgenden werden die Schaltflächen kurz beschrieben:

- **Weiter** – Aktion bestätigen und zum folgenden Schritt des Installationsvorgangs weitergehen.
- **Zurück** – zum vorherigen Schritt der Installation zurückkehren.
- **Abbrechen** – Installation des Produkts abbrechen.
- **Fertig** – Vorgang zur Programminstallation auf dem Computer fertig stellen.

Betrachten wir die einzelnen Schritte des Installationsvorgangs ausführlich.

In diesem Abschnitt

Schritt 1. Suche nach einer neueren Programmversion 41
Schritt 2. Überprüfen des Systems auf die Installationsvoraussetzungen 42
Schritt 3. Startfenster des Installationsassistenten 42
Schritt 4. Lesen des Lizenzvertrags.. 42
Schritt 5. Auswahl des Installationstyps.. 43
Schritt 6. Auswahl des Installationsordners 43
Schritt 7. Auswahl der zu installierenden Programmkomponenten..................... 44
Schritt 8. Suche nach anderen Antiviren-Programmen....................................... 45
Schritt 9. Abschließende Vorbereitungen für die Programminstallation 46
Schritt 10. Abschluss des Installationsvorgangs.. 46

Schritt 1. Suche nach einer neueren Programmversion

Bevor die Anwendung auf Ihrem Computer installiert wird, wird eine Verbindung zu den Kaspersky-Lab-Updateservern aufgebaut und geprüft, ob eine neuere Version der zur Installation vorgesehenen Anwendung verfügbar ist.

Wenn auf den Kaspersky-Lab-Updateservern keine neuere Version des Programms gefunden wird, wird der Installationsassistent der vorliegenden Version gestartet.

Wenn eine neuere Programmversion auf den Updateservern vorhanden ist, wird Ihnen angeboten, sie herunterzuladen und auf Ihrem Computer zu installieren. Bei Ablehnung der neueren Version wird der Installationsassistent der vorliegenden Version gestartet. Wenn Sie entscheiden, die neuere Version zu installieren, werden die Distributionsdateien auf Ihren Computer kopiert und der Installationsassistent der neuen Version wird automatisch gestartet. Das weitere Vorgehen zur Installation einer neueren Version entnehmen Sie bitte der Dokumentation der entsprechenden Programmversion.

Schritt 2. Überprüfen des Systems auf die Installationsvoraussetzungen

Bevor das Programm auf Ihrem Computer installiert wird, werden das installierte Betriebssystem und die vorhandenen Service Packs auf Übereinstimmung mit den Softwarevoraussetzungen für die Installation überprüft (s. Abschnitt “Hardware- und Softwarevoraussetzungen” auf S. 14). Außerdem wird überprüft, ob die erforderlichen Programme auf Ihrem Computer vorhanden sind und ob Sie über die zur Programminstallation notwendigen Rechte verfügen.

Sollte eine bestimmte Voraussetzung nicht erfüllt sein, dann erscheint eine entsprechende Meldung auf dem Bildschirm. Es wird empfohlen, vor der Installation der Kaspersky-Lab-Anwendung die erforderlichen Programme und mit Hilfe des Diensts **Windows Update** die fehlenden Service Packs zu installieren.

Schritt 3. Startfenster des Installationsassistenten

Wenn Ihr System die Voraussetzungen vollständig erfüllt (s. Abschnitt “Hardware- und Softwarevoraussetzungen” auf S. 14), keine neuere Programmversion auf den Kaspersky-Lab-Updateservern gefunden wurde oder Sie die Installation einer neueren Version abgelehnt haben, wird auf Ihrem Computer der Installationsassistent der vorliegenden Programmversion gestartet. Auf dem Bildschirm wird das Startfenster des Installationsassistenten geöffnet. Es enthält Informationen über den Beginn der Programminstallation auf Ihrem Computer.

Klicken Sie auf **Weiter**, um die Installation fortzusetzen. Klicken Sie auf **Abbrechen**, um die Installation zu verwerfen.

Schritt 4. Lesen des Lizenzvertrags

Das folgende Fenster des Installationsprogramms enthält den Lizenzvertrag, der zwischen Ihnen und Kaspersky Lab geschlossen wird. Bitte lesen Sie den

Vertrag aufmerksam. Wenn Sie allen Punkten des Vertrags zustimmen, wählen Sie die Variante **Ich akzeptiere die Bedingungen des Lizenzvertrags** und klicken Sie auf die Schaltfläche **Weiter**. Die Installation wird fortgesetzt.

Klicken Sie auf **Abbrechen**, um die Installation zu verwerfen.

SCHRITT 5. AUSWAHL DES INSTALLATIONSTYPS

Auf dieser Etappe können Sie eine geeignete Methode für die Installation der Anwendung wählen:

- **Schnelle Installation**. Bei Auswahl dieser Variante wird die Anwendung vollständig auf Ihrem Computer installiert und die von den Kaspersky-Lab-Spezialisten empfohlenen Einstellungen werden verwendet. Am Ende der Installation wird der Konfigurationsassistent der Anwendung gestartet.
- **Benutzerdefinierte Installation**. In diesem Fall können Sie wählen, welche Programmkomponenten auf dem Computer installiert werden sollen, und den Installationsordner festlegen (s. Abschnitt “Schritt 6. Auswahl des Installationsordners” auf S. 43). Außerdem können Sie mit Hilfe eines speziellen Assistenten die Anwendung aktivieren und konfigurieren.

Bei Auswahl der ersten Variante geht der Installationsassistent sofort zu Schritt 8 über (s. Abschnitt “Schritt 8. Suche nach anderen Antiviren-Programmen” auf S. 45). Im zweiten Fall ist auf jeder Installationsetappe die Eingabe oder Bestätigung bestimmter Daten durch den Benutzer erforderlich.

SCHRITT 6. AUSWAHL DES INSTALLATIONSORDNERS

> Hinweis
>
> Dieser Schritt des Installationsassistenten wird nur bei der benutzerdefinierten Programminstallation ausgeführt (s. Abschnitt “Schritt 5. Auswahl des Installationstyps” auf S. 43).

Auf dieser Etappe können Sie einen Ordner auf Ihrem Computer wählen, in dem die Anwendung installiert werden soll. Der Standardpfad lautet:

- **<Laufwerk> \ Programme \ Kaspersky Lab \ Kaspersky Internet Security 2009** – für 32-Bit-Systeme.
- **<Laufwerk> \ Programme (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2009** – für 64-Bit-Systeme.

Sie können einen anderen Ordner wählen. Klicken Sie dazu auf die Schaltfläche **Durchsuchen** und wählen Sie im standardmäßigen Auswahlfenster einen Ordner aus oder geben Sie den Pfad des Ordners im entsprechenden Eingabefeld an.

Achtung!

Falls Sie den vollständigen Pfad des Ordners manuell angeben, beachten Sie, dass er aus maximal 200 Zeichen bestehen und keine Sonderzeichen enthalten darf.

Klicken Sie auf **Weiter**, um die Installation fortzusetzen.

SCHRITT 7. AUSWAHL DER ZU INSTALLIERENDEN PROGRAMMKOMPONENTEN

Dieser Schritt des Installationsassistenten wird nur bei der benutzerdefinierten Programminstallation ausgeführt (s. Abschnitt “Schritt 5. Auswahl des Installationstyps” auf S. 43).

Bei der benutzerdefinierten Installation müssen Sie die Programmkomponenten festlegen, die auf Ihrem Computer installiert werden sollen. Standardmäßig sind alle Programmkomponenten zur Installation vorgesehen: Schutzkomponenten, Untersuchungsaufgaben und Update.

Bei der Entscheidung, welche Komponenten Sie installieren möchten, kann die jeweilige Kurzbeschreibung hilfreich sein. Wenn Sie eine Komponente in der Liste auswählen, finden Sie unten im Feld die entsprechenden Informationen. Die Informationen enthalten eine Kurzbeschreibung der Funktion der Komponente und nennen den für ihre Installation auf der Festplatte erforderlichen Platz.

Um die Installation einer Komponente abzulehnen, öffnen Sie das Kontextmenü auf dem Symbol, das sich neben dem Namen der Komponente befindet, und wählen Sie den Punkt **Die Komponente wird nicht verfügbar sein**. Beachten Sie, dass Sie auf den Schutz vor einer ganzen Reihe gefährlicher Programme verzichten, wenn Sie eine bestimmte Komponente nicht installieren.

Um eine Komponente zur Installation auszuwählen, öffnen Sie das Kontextmenü auf dem Symbol, das sich neben dem Namen der Komponente befindet, und wählen Sie den Punkt **Die Komponente wird auf der lokalen Festplatte installiert**.

Klicken Sie auf die Schaltfläche **Weiter**, nachdem Sie die zur Installation gewünschten Komponenten gewählt haben. Um zur Liste der standardmäßig zur Installation vorgesehenen Komponenten zurückzukehren, klicken Sie auf die Schaltfläche **Zurücksetzen**.

SCHRITT 8. SUCHE NACH ANDEREN ANTIVIREN-PROGRAMMEN

Auf dieser Etappe erfolgt die Suche nach anderen auf Ihrem Computer installierten Antiviren-Produkten (einschließlich Kaspersky-Lab-Produkte), deren gleichzeitige Verwendung mit der Anwendung zu Konflikten führen kann.

Wenn auf Ihrem Computer solche Programme gefunden werden, werden Sie auf dem Bildschirm aufgelistet. Sie werden aufgefordert, diese Programme zu löschen, bevor die Installation fortgesetzt wird.

Unter der Liste der gefundenen Antiviren-Anwendungen können Sie wählen, ob sie automatisch oder manuell entfernt werden sollen.

Wenn sich unter den gefundenen Antiviren-Programmen eine Kaspersky-Lab-Anwendung der Version 7.0 befindet, wird bei manueller Deinstallation empfohlen, díe zur Arbeit dieser Anwendung verwendete Schlüsseldatei zu speichern. Der vorhandene Schlüssel kann für die neue Version der Anwendung verwendet werden. Außerdem wird empfohlen, die Quarantäne- und Backup-Objekte zu speichern. Diese Objekte werden automatisch in die Quarantäne der neuen Anwendungsversion verschoben und Sie können damit weiterarbeiten.

Bei der automatischen Deinstallation der Anwendungsversion 7.0 werden die Aktivierungsdaten vom Programm gespeichert und bei der Installation der Version 2009 übernommen.

Achtung!

Die Anwendung unterstützt Schlüsseldateien für Version 6.0 und 7.0. Schlüssel, die zu Anwendungen der Version 5.0 passen, werden nicht unterstützt.

Klicken Sie auf **Weiter**, um die Installation fortzusetzen.

Schritt 9. Abschließende Vorbereitungen für die Programminstallation

Auf dieser Etappe können Sie die Programminstallation auf Ihrem Computer abschließend vorbereiten.

Bei der erstmaligen und bei der benutzerdefinierten Installation der Anwendung (s. Abschnitt “Schritt 5. Auswahl des Installationstyps” auf S. 43) sollte das Kontrollkästchen Schutz für Module vor dem Installationsbeginn aktivieren nicht entfernt werden. Sollten bei der Installation der Anwendung Fehler auftreten, dann erlaubt der aktivierte Modulschutz, die Installation auf korrekte Weise rückgängig zu machen. Bei einem wiederholten Versuch zur Installation der Anwendung wird empfohlen, dieses Kontrollkästchen zu deaktivieren.

Hinweis

Wird die Anwendung im Remote-Modus über **Windows Remote Desktop** auf dem Computer installiert, dann ist es ratsam, das Kontrollkästchen **Schutz für Module vor dem Installationsbeginn aktivieren** zu deaktivieren. Andernfalls besteht die Möglichkeit, dass der Installationsvorgang nicht oder fehlerhaft durchgeführt wird.

Klicken Sie auf **Weiter**, um die Installation fortzusetzen. Die Dateien der Anwendungsdistribution werden nun auf Ihren Computer kopiert.

Achtung!

Bei der Installation von Komponenten, die der Überwachung des Netzwerkverkehrs dienen, werden bestehende Netzwerkverbindungen getrennt. Die Mehrzahl der getrennten Verbindungen wird nach einiger Zeit wiederhergestellt.

Schritt 10. Abschluss des Installationsvorgangs

Das Fenster **Installation fertig stellen** enthält Informationen über den Abschluss des Installationsvorgangs der Anwendung auf Ihrem Computer.

Wenn zum korrekten Fertigstellen der Programminstallation ein Neustart des Computers erforderlich sein sollte, erscheint eine entsprechende Meldung auf

dem Bildschirm. Nach dem Neustart des Systems wird automatisch der Konfigurationsassistent gestartet.

Wenn zum Fertigstellen der Installation kein Systemneustart erforderlich ist, klicken Sie auf die Schaltfläche **Weiter**, um zum Konfigurationsassistenten der Anwendung zu gelangen.

PROGRAMMOBERFLÄCHE

Die Anwendung verfügt über eine intuitiv bedienbare und komfortable Oberfläche. In diesem Kapitel werden die wichtigsten Elemente der Oberfläche ausführlich beschrieben.

Neben der Hauptoberfläche bietet das Programm auch Erweiterungskomponenten (Plug-ins), die in die Programme Microsoft Office Outlook (Viren- und Spam-Untersuchung), Microsoft Outlook Express (Windows Mail), The Bat! (Viren- und Spam-Untersuchung), Microsoft Internet Explorer und Microsoft Windows Explorer integriert werden können. Die Plug-ins erweitern die Möglichkeiten der genannten Programme, weil die Steuerung und Konfiguration der Komponenten **Mail-Anti-Virus** und **Anti-Spam** direkt aus ihrem Interface möglich ist.

IN DIESEM ABSCHNITT

Symbol im Infobereich der Taskleiste 48

Kontextmenü 49

Programmhauptfenster 51

Meldungen 54

Programmkonfigurationsfenster 54

SYMBOL IM INFOBEREICH DER TASKLEISTE

Sofort nach der Installation des Programms erscheint sein Symbol im Infobereich der Taskleiste von Microsoft Windows.

Das Symbol ist ein Indikator für die Arbeit des Programms. Es informiert über den Schutzstatus und visualisiert eine Reihe wichtiger Aktionen, die vom Programm ausgeführt werden.

Wenn das Symbol aktiv (farbig) ist, bedeutet es, dass der Schutz komplett aktiviert ist oder bestimmte Schutzkomponenten arbeiten. Wenn das Symbol inaktiv (schwarzweiß) ist, dann sind alle Schutzkomponenten deaktiviert.

Abhängig von der ausgeführten Operation ändert sich das Aussehen des Symbols:

– Eine E-Mail-Nachricht wird untersucht.

– Das Update der Datenbanken und Programm-Module wird ausgeführt.

– Der Computer muss neu gestartet werden, um Updates zu übernehmen.

– Bei der Arbeit einer Komponente der Anwendung ist eine Störung aufgetreten.

Das Symbol bietet außerdem Zugriff auf die wichtigsten Elemente der Programmoberfläche: Kontextmenü (s. Abschnitt “Kontextmenü” auf S. 49) und Hauptfenster (s. Abschnitt “Programmhauptfenster” auf S. 51).

Um das Kontextmenü zu öffnen, klicken Sie mit der rechten Maustaste auf das Programmsymbol.

Um das Programmhauptfenster zu öffnen, doppelklicken Sie mit der linken Maustaste auf das Programmsymbol. Das Hauptfenster wird immer im Abschnitt **Schutz** geöffnet.

Wenn Nachrichten von Kaspersky Lab erscheinen, wird im Infobereich der Taskleiste von Microsoft Windows das Symbol eingeblendet. Durch Doppelklick mit der linken Maustaste auf das Symbol wird ein Fenster mit dem Nachrichtentext geöffnet.

KONTEXTMENÜ

Das Kontextmenü bietet Zugriff auf die wichtigsten Schutzaufgaben.

Das Menü des Programms enthält folgende Punkte:

- **Update** – Starten der Aktualisierung der Datenbanken und Module des Programms und der Installation der Updates auf Ihrem Computer.
- **Vollständige Untersuchung des Computers** – Starten der vollständigen Untersuchung des Computers auf das Vorhandensein von schädlichen Objekten. Dabei werden die Objekte auf allen Laufwerken einschließlich der Wechseldatenträger untersucht.
- **Auf Viren untersuchen** – Zur Auswahl von Objekten und zum Start der Virensuche wechseln. In der Grundeinstellung enthält die Liste eine Reihe von Objekten wie beispielsweise den Ordner **Eigene Dateien** und Mailboxen. Sie können die Liste ergänzen, Untersuchungsobjekte wählen und die Virensuche starten.
- **Netzwerkmonitor** – Liste der aktiven Netzwerkverbindungen, der offenen Ports und des Datenverkehrs anzeigen.
- **Virtuelle Tastatur** – Zu der virtuellen Tastatur wechseln.

- **Kaspersky Internet Security** – Programmhauptfenster öffnen (s. Abschnitt “Programmhauptfenster” auf S. 51).
- **Aktivierung** – Zur Aktivierung des Programms wechseln. Um den Status eines registrierten Benutzers zu erhalten, muss Ihre Version des Programms aktiviert werden. Dieser Menüpunkt ist nur vorhanden, wenn das Programm noch nicht aktiviert wurde.
- **Einstellungen** – Zur Ansicht und zum Anpassen der Funktionsparameter des Programms wechseln.
- **Über das Programm** – Fenster mit Informationen über das Programm öffnen.
- **Schutz anhalten / Schutz fortsetzen** – Arbeit der Echtzeitschutz-Komponenten vorübergehend deaktivieren / aktivieren. Dieser Menüpunkt bezieht sich nicht auf das Programm-Update und die Ausführung von Aufgaben zur Virensuche.
- **Netzwerkverkehr blockieren** – Alle Netzwerkverbindungen des Computers vorübergehend sperren. Um die Interaktion des Computers mit dem Netzwerk wieder zu erlauben, wählen Sie erneut diesen Punkt des Kontextmenüs.
- **Beenden** – Arbeit des Programms beenden (bei Auswahl dieses Menüpunkts wird das Programm aus dem Arbeitsspeicher des Computers ausgeladen).

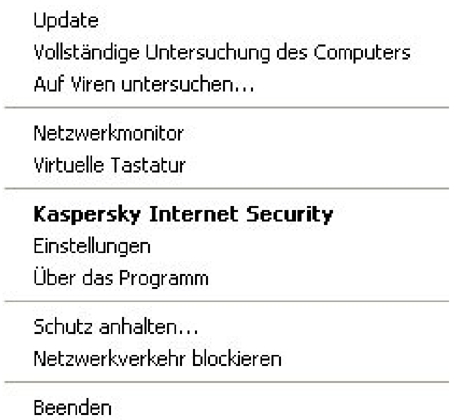


Abbildung 1: Kontextmenü

Wird das Kontextmenü geöffnet, während eine Aufgabe zur Virensuche läuft, so wird ihr Name mit Prozentangabe des Ausführungsergebnisses im Kontextmenü angezeigt. Durch die Auswahl der Aufgabe gelangen Sie in das Hauptfenster mit einem Bericht über ihre aktuellen Ausführungsergebnisse.

PROGRAMMHAUPTFENSTER

Das Hauptfenster lässt sich bedingt in drei Bereiche aufteilen:

- Der obere Bereich des Fensters informiert über den aktuellen Schutzstatus Ihres Computers.



Abbildung 2: Aktueller Schutzstatus des Computers

  Es existieren drei Möglichkeiten für den Zustand des Schutzes. Jeder Zustand wird anschaulich durch eine bestimmte Farbe dargestellt. Die Farben entsprechen den Signalen einer Verkehrsampel. Grün bedeutet, dass der Schutz Ihres Computers dem erforderlichen Niveau entspricht. Gelb und Rot signalisieren, dass in den Einstellungen oder bei der Arbeit des Programms bestimmte Sicherheitsbedrohungen vorliegen. Als Bedrohung gilt nicht nur der Fund schädlicher Programme, sondern auch die Verwendung veralteter Datenbanken, die deaktivierte Schutzkomponenten, die Auswahl einer niedrigen Sicherheitsstufe u.a.

  Vorhandene Sicherheitsrisiken sollten umgehend behoben werden. Verwenden Sie den Link **Korrigieren** (s. Bild oben), um ausführliche Informationen darüber zu erhalten und die Bedrohungen schnell zu beheben.

- Die linke Seite des Fensters erlaubt es, schnell und bequem zu einer beliebigen Funktion, zur Ausführung von Untersuchungsaufgaben, zum Update und anderen Optionen zu gelangen.

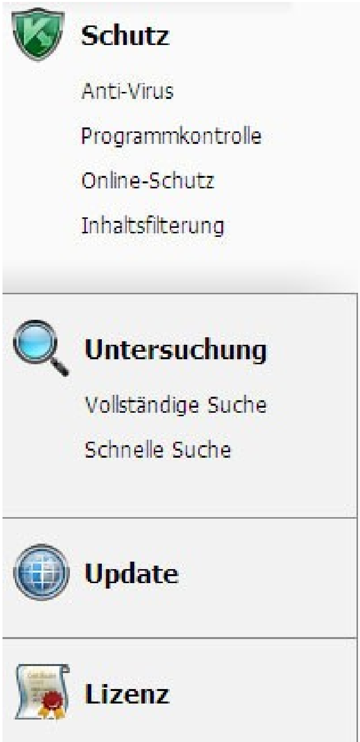


Abbildung 3: Linke Seite des Hauptfensters

- Die rechte Seite des Fensters enthält Informationen über die auf der linken Seite gewählte Programmfunktion, erlaubt es, die Parameter aller Funktionen anzupassen, bietet Werkzeuge zum Ausführen von Aufgaben zur Virensuche, zum Update-Download, u.a.

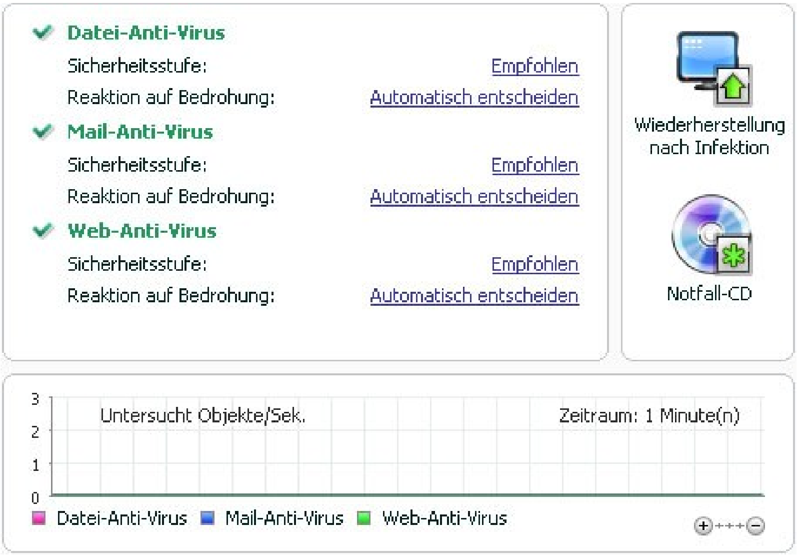


Abbildung 4: Infobereich des Hauptfensters

Außerdem stehen folgende Schaltflächen zur Verfügung:

- **Einstellungen** – in das Konfigurationsfenster des Programms wechseln.
- **Hilfe** – Zum Hilfesystem des Programms wechseln.
- **Gefunden** – Öffnen einer Liste der gefährlichen Objekte, die bei der Arbeit einer Komponente oder bei der Ausführung einer Untersuchungsaufgabe gefunden wurden, sowie Anzeige einer ausführlichen Statistik über die Arbeitsergebnisse des Programms.
- **Berichte** – Zu einer Liste der Ereignisse, die bei der Arbeit des Programms eingetreten sind, wechseln.
- **Support** – Ein Fenster mit Informationen über das System und mit Links zu Informationsressourcen von Kaspersky Lab (Webseite des Technischen Supports, Forum) öffnen.

> Hinweis
>
> Sie können das Aussehen des Programms anpassen, indem Sie grafische Elemente und Farbschemen erstellen und verwenden.

MELDUNGEN

Wenn bei der Arbeit des Programms Ereignisse eintreten, werden auf dem Bildschirm spezielle Meldungen eingeblendet: Popupmeldungen über dem Programmsymbol im Infobereich der Taskleiste von Microsoft Windows.

In Abhängigkeit davon, welche Relevanz das Ereignis für die Computersicherheit besitzt, sind folgende Arten von Meldungen möglich:

- **Alarm**. Ein Ereignis mit kritischer Priorität ist eingetreten. Beispiele: "Ein Virus wurde gefunden" oder "Im System wurde gefährliche Aktivität erkannt". Die sofortige Entscheidung über das weitere Vorgehen ist erforderlich. Dieser Meldungstyp besitzt die Farbe Rot.
- **Achtung**. Ein potentiell gefährliches Ereignis hat sich ereignet. Beispiele: "Ein möglicherweise infiziertes Objekt wurde gefunden" oder "Im System wurde verdächtige Aktivität erkannt". Es muss entschieden werden, inwieweit das Ereignis nach Ihrem Ermessen gefährlich ist. Dieser Meldungstyp besitzt die Farbe Gelb.
- **Hinweis**. Die Meldung informiert über ein Ereignis, das keine vorrangige Priorität besitzt. Zu diesem Typ zählen beispielsweise Meldungen, die bei der Arbeit der Komponente **Inhaltsfilterung** vorkommen. Dieser Meldungstyp besitzt die Farbe Grün.

PROGRAMMKONFIGURATIONSFENSTER

Das Programmkonfigurationsfenster kann aus dem Hauptfenster (s. Abschnitt "Programmhauptfenster" auf S. 51) oder aus dem Kontextmenü (s. Abschnitt auf “Kontextmenü” S. 49) des Programms geöffnet werden. Klicken Sie dazu im oberen Bereich des Hauptfensters auf den Link **Einstellungen** oder wählen Sie den gleichnamigen Punkt im Kontextmenü des Programms.

Das Konfigurationsfenster besteht aus zwei Teilen:

- Die linke Seite des Fensters bietet Zugriff auf Programmkomponenten, Untersuchungs- und Updateaufgaben und andere Funktionen.
- Die rechte Seite des Fensters enthält eine Liste von Parametern für die auf der linken Seite ausgewählte Komponente, Aufgabe usw.

ERSTE SCHRITTE

Bei der Entwicklung von Kaspersky Internet Security bestand für die Kaspersky-Lab-Spezialisten eine der Hauptaufgaben in der optimalen Konfiguration aller Programmeinstellungen. Das verleiht einem Benutzer unabhängig von seiner Erfahrung mit Computern die Möglichkeit, sofort nach der Programminstallation die Sicherheit des Computers zu gewährleisten, ohne sich weiter mit den Einstellungen zu beschäftigen.

Um die Benutzerfreundlichkeit zu erhöhen, wurden die Schritte zur grundlegenden Konfiguration in einem Konfigurationsassistenten zusammengefasst, der am Ende der Programminstallation gestartet wird. Mit Unterstützung des Assistenten können Sie das Programm aktivieren, die Updateparameter anpassen, den Zugriff auf die Anwendung mit Hilfe eines Kennworts beschränken und andere Einstellungen vornehmen.

Es besteht die Möglichkeit, dass Ihr Computer vor der Installation der Anwendung von Schadprogrammen infiziert wurde. Um bereits vorhandene Malware zu finden, starten Sie die Untersuchung des Computers (s. Abschnitt “Virenuntersuchung des Computers” auf S. 58).

Durch Aktionen schädlicher Programme und Systemabstürze können die Einstellungen Ihres Computers beschädigt werden. Starten Sie den Assistenten zur Sicherheitsanalyse (s. Abschnitt “Sicherheitsanalyse” auf S. 57), um die installierten Programme nach Schwachstellen und die Systemeinstellungen nach Anomalien zu durchsuchen.

Die im Lieferumfang enthaltenen Datenbanken können zum Zeitpunkt der Programminstallation veraltet sein. Starten Sie das Programm-Update (s. S. 57) (sofern das Update nicht mit Hilfe des Konfigurationsassistenten oder sofort nach der Installation automatisch erfolgt ist).

Die Programmkomponente Anti-Spam verwendet einen lernfähigen Algorithmus zum Erkennen unerwünschter E-Mails. Starten Sie den Trainingsassistenten für Anti-Spam, um die Komponente für die Arbeit mit Ihren E-Mails einzustellen.

Nach den oben beschriebenen Aktionen ist die Anwendung zur Arbeit bereit. Verwenden Sie den Assistenten zu Sicherheitsverwaltung, um das Schutzniveau Ihres Computers zu beurteilen (s. Abschnitt "Sicherheitsverwaltung" auf S. 59).

IN DIESEM ABSCHNITT

Auswahl des Netzwerktyps 56
Programm-Update 57
Sicherheitsanalyse 57
Virenuntersuchung des Computers 58
Teilnahme an Kaspersky Security Network 58
Sicherheitsverwaltung 59
Schutz anhalten 61

AUSWAHL DES NETZWERKTYPS

Nach der Programminstallation überwacht die Komponente Firewall die aktiven Netzwerkverbindungen auf Ihrem Computer. Jede Netzwerkverbindung erhält einen Status, der die erlaubte Netzwerkaktivität festlegt.

Wenn Sie für Kaspersky Internet Security den interaktiven Funktionsmodus gewählt haben, wird beim Fund einer Netzwerkverbindung eine Meldung angezeigt. Im Meldungsfenster können Sie den Status des neuen Netzwerks festlegen:

- **Öffentliches Netzwerk** – Für Netzwerkverbindungen mit diesem Status wird der externe Zugriff auf Ihren Computer verboten. In einem solchen Netzwerk ist auch der Zugriff auf gemeinsame Ordner und Drucker untersagt. Es wird empfohlen, dem Internet diesen Status zuzuweisen.
- **Lokales Netzwerk** – Für Netzwerkverbindungen mit diesem Status wird der Zugriff auf gemeinsame Ordner und Netzwerkdrucker erlaubt. Es wird empfohlen, diesen Status für ein geschütztes lokales Netzwerk (z.B. Firmennetzwerk) zu verwenden.
- **Vertrauenswürdiges Netzwerk** – Für Netzwerkverbindungen mit diesem Status wird jede Aktivität erlaubt. Dieser Status wird nur für eine absolut sichere Zone empfohlen.

Der Lieferumfang von Kaspersky Internet Security enthält für jeden Netzwerkstatus eine Auswahl von Regeln zur Steuerung der Netzwerkaktivität. Der Status, der einem Netzwerk zugewiesen wird, wenn es zum ersten Mal gefunden wird, kann später geändert werden.

PROGRAMM-UPDATE

Achtung!

Für das Update von Kaspersky Internet Security ist eine bestehende Internetverbindung erforderlich.

Zum Lieferumfang von Kaspersky Internet Security gehören Datenbanken mit Bedrohungssignaturen, Muster von typischen Spam-Phrasen und Beschreibungen von Netzwerkangriffen. Zum Zeitpunkt der Programminstallation können die Datenbanken verwaltet sein, weil die Datenbanken und Programm-Module regelmäßig von Kaspersky Lab aktualisiert werden.

Im Rahmen des Konfigurationsassistenten für das Programm können Sie einen Startmodus für das Update wählen. Kaspersky Internet Security überprüft in der Grundeinstellung automatisch, ob auf den Kaspersky-Lab-Servern neue Updates vorhanden sind. Wenn auf dem Server neue Updates bereitstehen, führt Kaspersky Internet Security im Hintergrundmodus den Download und die Installation der Updates durch.

Um den Schutz Ihres Computers aktuell zu halten, wird empfohlen, Kaspersky Internet Security sofort nach der Installation zu aktualisieren.

- *Um Kaspersky Internet Security manuell zu aktualisieren:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
  3. Klicken Sie auf die Schaltfläche **Update starten**.

SICHERHEITSANALYSE

Aufgrund unerwünschter Aktivität auf Ihrem Computer, die durch Systemabstürze oder Aktivität schädlicher Programme verursacht werden kann, können die Einstellungen des Betriebssystems beschädigt werden. Außerdem können die auf Ihrem Computer installierten Anwendungen Schwachstellen aufweisen, die es Angreifern ermöglichen, Ihren Computer zu beschädigen.

Um derartige Sicherheitsprobleme zu erkennen und zu beheben, empfehlen die Kaspersky-Lab-Spezialisten, nach der Installation der Anwendung den Assistenten zur Sicherheitsanalyse zu starten. Der Assistent zur Sicherheitsanalyse führt in den installierten Anwendungen die Suche nach Schwachstellen durch und sucht in den Einstellungen des Betriebssystems und des Browsers nach Beschädigungen und Anomalien.

Um den Assistenten zu starten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Seite des Fensters den Abschnitt **Programmkontrolle**.
3. Starten Sie die Aufgabe **Sicherheitsanalyse**.

VIRENUNTERSUCHUNG DES COMPUTERS

Die Autoren schädlicher Programme geben sich große Mühe, die Aktivität ihrer Programme zu verheimlichen. Deshalb kann es sein, dass Sie die Existenz von Malware auf Ihren Computer nicht bemerken.

Bei der Installation der Anwendung wird automatisch die Aufgabe **Schnelle Suche** ausgeführt. Diese Aufgabe dient der Suche und Neutralisierung von schädlichen Programmen in Objekten, die beim Hochfahren des Betriebssystems geladen werden.

Die Spezialisten von Kaspersky Lab empfehlen, zusätzlich die Aufgabe **Vollständige Suche** auszuführen.

Um eine Untersuchungsaufgabe zu starten / zu beenden:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie auf die Schaltfläche **Untersuchung starten**, um die Untersuchung zu starten. Klicken Sie auf die Schaltfläche **Untersuchung beenden**, um die Ausführung einer laufenden Aufgabe zu beenden.

TEILNAHME AN KASPERSKY SECURITY NETWORK

Jeden Tag taucht eine Vielzahl neuer Bedrohungen auf. Um das Erstellen einer Statistik über neue Bedrohungstypen und ihre Quellen sowie die Entwicklung entsprechender Neutralisierungsmethoden zu beschleunigen, bietet Kaspersky Lab Ihnen die Teilnahme an dem Dienst Kaspersky Security Network an.

Bei der Verwendung von Kaspersky Security Network werden folgende Informationen an Kaspersky Lab gesendet:

- Unikaler Identifikator, den die Anwendung Ihrem Computer zugewiesen hat. Dieser Identifikator charakterisiert die Hardwareparameter Ihres Computers und enthält keinerlei persönliche Informationen.
- Informationen über Bedrohungen, die von den Anwendungskomponenten gefunden wurden. Die Auswahl der Informationen ist vom Typ der gefundenen Bedrohung abhängig.
- Informationen zum System: Version des Betriebssystems, installierte Service Packs, geladene Dienste und Treiber, Versionen von Browsern und Mailprogrammen, Erweiterungen für Browser, Versionsnummer der installierten Kaspersky-Lab-Anwendung.

Im Rahmen von Kaspersky Security Network wird außerdem eine erweiterte Statistik erstellt. Dazu gehören Informationen über:

- auf Ihrem Computer geladene ausführbare Dateien und signierte Anwendungen,
- auf Ihrem Computer gestartete Anwendungen.

Die statistischen Informationen werden gesendet, wenn das Programm-Update abgeschlossen wird.

> Achtung!
>
> Kaspersky Lab garantiert, dass im Rahmen von Kaspersky Security Network keine persönlichen Benutzerdaten gesammelt und gesendet werden.

► *Um die Parameter für das Senden der Statistik anzupassen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Feedback**.
3. Aktivieren Sie das Kontrollkästchen **Ich bin mit der Teilnahme an Kaspersky Security Network einverstanden**, um die Teilnahme an Kaspersky Security Network zu bestätigen. Aktivieren Sie das Kontrollkästchen **Ich bin einverstanden, dass im Rahmen von Kaspersky Security Network eine erweiterte Statistik gesendet wird**, um die Ihr Einverständnis mit dem Senden einer erweiterten Statistik zu erklären.

SICHERHEITSVERWALTUNG

Über das Auftreten von Problemen im Computerschutz informiert der Schutzstatus des Computers (s. Abschnitt “Programmhauptfenster” auf S. 51)

durch eine Veränderung der Farbe des Schutzstatussymbols und der Leiste, auf der sich das Symbol befindet. Wenn im Schutz Probleme auftreten, sollten diese umgehend behoben werden.



Abbildung 5: Aktueller Schutzstatus des Computers

Über den Link **Korrigieren** (s. Bild oben) gelangen Sie zu der Registerkarte **Status** (s. Bild unten), die eine Liste der aufgetretenen Probleme und entsprechende Lösungsmöglichkeiten bietet.

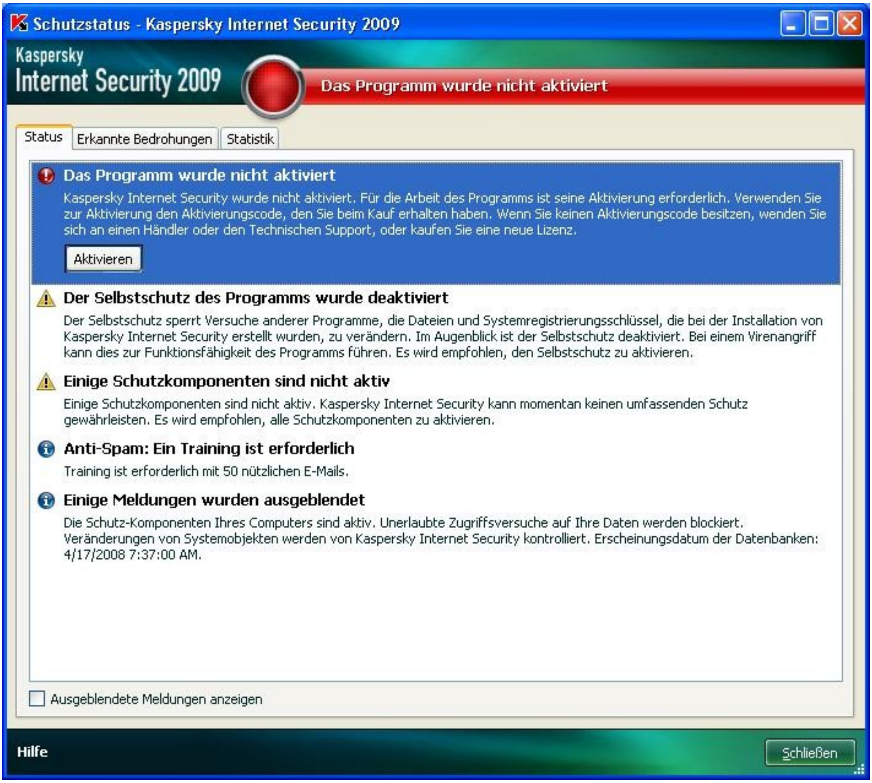


Abbildung 6: Beheben von Sicherheitsproblemen

Sie können eine Liste der vorhandenen Probleme ansehen. Die Reihenfolge der Probleme entspricht der Priorität, nach der sie gelöst werden sollten: Zu Beginn stehen die wichtigsten Probleme mit rotem Statussymbol, danach folgen die

weniger wichtigen mit gelbem Statussymbol und zum Schluss informative Meldungen. Für jedes Problem ist eine ausführliche Beschreibung vorhanden und folgende Aktionen werden angeboten:

- *Sofort beheben*. Mit Hilfe der entsprechenden Schaltflächen können Sie zur sofortigen Neutralisierung der Probleme übergehen, was der empfohlenen Aktion entspricht.
- *Behebung aufschieben*. Wenn das sofortige Beheben eines Problems aufgrund bestimmter Umstände nicht möglich ist, kann diese Aktion aufgeschoben werden und Sie können später dazu zurückkehren. Verwenden Sie dazu die Schaltfläche **Meldung ausblenden**.

  Beachten Sie, dass diese Möglichkeit für kritische Probleme nicht vorgesehen ist. Dazu gehören beispielsweise die Existenz nicht neutralisierter schädlicher Objekte, Störungen bei der Arbeit einer oder mehrerer Komponenten, und beschädigte Programmdateien.

Um Meldungen, die zuvor ausgeblendet wurden, erneut in der Liste anzuzeigen, aktivieren Sie das Kontrollkästchen **Ausgeblendete Meldungen anzeigen**.

SCHUTZ ANHALTEN

Das Anhalten des Schutzes bedeutet, dass alle Schutzkomponenten für einen bestimmten Zeitraum deaktiviert werden.

- *Um den Schutz des Computers anzuhalten:*

1. Wählen Sie im Kontextmenü des Programms den Punkt **Schutz anhalten** (s. Abschnitt “Kontextmenü” auf S. 49).
2. Wählen Sie im folgenden Fenster zum Deaktivieren des Schutzes den Zeitraum, nach dem der Schutz wieder aktiviert werden soll:
   - **In <Zeitraum>** – Der Schutz wird nach Ablauf des festgelegten Zeitraums wieder aktiviert. Wählen Sie in der Dropdown-Liste einen Wert für den Zeitraum aus.
   - **Nach dem Neustart** – Der Schutz wird nach dem Neustart des Systems aktiviert (unter der Bedingung, dass der Modus zum Programmstart beim Hochfahren des Systems aktiviert ist).
   - **Manuell** – Der Schutz wird erst dann wieder aktiviert, wenn Sie ihn starten. Wählen Sie den Punkt **Schutz fortsetzen** im Kontextmenü des Programms, um den Schutz zu aktivieren.

Durch das vorübergehende Deaktivieren wird die Arbeit aller Schutz-Komponenten angehalten. Darüber informieren:

- Die inaktiven (grauen) Namen der deaktivierten Komponenten im Abschnitt **Schutz** des Hauptfensters.
- Das inaktive (graue) Programmsymbol im Infobereich der Taskleiste (s. Abschnitt “Symbol im Infobereich der Taskleiste” auf S. 48).
- Rote Farbe des Statussymbols und der Leiste im Programmhauptfenster.

Wenn im Augenblick, in dem der Schutz angehalten wurde, Netzwerkverbindungen vorhanden waren, dann erscheint auf dem Bildschirm eine Datenstromüberwachung.

ÜBERPRÜFUNG DER PROGRAMMEINSTELLUNGEN

Nach der Installation und Konfiguration der Anwendung können Sie mit Hilfe eines "Testvirus" und dessen Modifikationen prüfen, ob die Einstellungen korrekt sind. Die Prüfung muss für jede Schutzkomponente und für jedes Protokoll einzeln ausgeführt werden.

IN DIESEM ABSCHNITT

EICAR-"Testvirus" und seine Modifikationen 63

Testen des Schutzes für HTTP-Datenverkehr 67

Testen des Schutzes für SMTP-Datenverkehr 67

Überprüfung der Einstellungen von Datei-Anti-Virus 68

Überprüfung der Einstellungen für eine Aufgabe zur Virensuche 68

Überprüfung der Einstellungen für den Schutz vor unerwünschten E-Mails 69

EICAR-"TESTVIRUS" UND SEINE MODIFIKATIONEN

Dieser "Testvirus" wurde von dem Institut eicar (The European Institute for Computer Antivirus Research) speziell zum Überprüfen der Arbeit von Antiviren-Produkten entwickelt.

Der "Testvirus" IST KEIN VIRUS und enthält keinen Programmcode, der Ihren Rechner beschädigen könnte. Trotzdem wird er von den meisten Antiviren-Softwareprodukten als Virus identifiziert.

Achtung!

Verwenden Sie nie echte Viren, um die Funktionsfähigkeit eines Antiviren-Produkts zu testen!

Der "Testvirus" kann von der offiziellen Internetseite des **EICAR**-Instituts heruntergeladen werden: http://www.eicar.org/anti_virus_test_file.htm.

Hinweis

Bevor der "Testvirus" heruntergeladen wird, muss der Antiviren-Schutz deaktiviert werden, weil die Datei *anti_virus_test_file.htm* andernfalls als infiziertes, mit dem HTTP-Protokoll übertragenes Objekt identifiziert und entsprechend behandelt wird.

Vergessen Sie nicht, den Antiviren-Schutz sofort nach dem Download des "Testvirus" wieder zu aktivieren.

Die von der Webseite des **EICAR**-Instituts heruntergeladene Datei wird vom Programm als infiziertes Objekt identifiziert, das einen Virus enthält, der **nicht desinfiziert werden kann**, und führt die für diesen Objekttyp festgelegte Aktion aus.

Um die Funktion des Programms zu prüfen, können Sie auch Modifikationen standardmäßigen "Testvirus" verwenden. Dazu wird der Inhalt des standardmäßigen "Testvirus" durch das Hinzufügen eines bestimmten Präfixes geändert (siehe Tabelle unten). Zum Erstellen von Modifikationen des "Testvirus" eignet sich ein beliebiger Text-Editor oder Hypertext-Editor wie beispielsweise **Microsoft Editor**, **UltraEdit32**, usw.

Achtung!

Die Prüfung der korrekten Funktion des Antiviren-Programms mit Hilfe eines modifizierten EICAR-"Testvirus" ist nur dann möglich, wenn die installierten Antiviren-Datenbanken nicht vor dem 24.10.2003 erschienen sind (kumulatives Update – Oktober 2003).

Die erste Spalte der Tabelle enthält Präfixe, die dem standardmäßigen "Testvirus" am Zeilenanfang hinzugefügt werden können. Die zweite Spalte zeigt die möglichen Werte für den Status, der einem Objekt aufgrund der Untersuchungsergebnisse von Anti-Virus zugewiesen werden kann. Die dritte Spalte bietet Informationen darüber, wie Objekte mit dem betreffenden Status vom Programm verarbeitet werden. Beachten Sie, dass die Aktionen für Objekte durch die Werte der Programmparameter bestimmt werden.

Nachdem dem "Testvirus" ein Präfix hinzugefügt wurde, speichern Sie die Datei z.B. unter dem Namen *eicar_dele.com*. Verwenden Sie die in der Tabelle angegebenen Namen für die modifizierten "Viren".

Tabelle 6. Modifikationen des "Testvirus"

Präfix	**Status des Objekts**	**Informationen zur Verarbeitung des Objekts**
Kein Präfix, standardmäßiger "Testvirus"	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt.
CORR–	**Beschädigt**.	Das Programm hat Zugriff auf das Objekt erhalten, kann es aber aufgrund einer Beschädigung nicht untersuchen (z.B. beschädigte Struktur des Objekts, ungültiges Dateiformat). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
WARN–	**Verdächtig**. Das Objekt enthält einen unbekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Objekt wurde bei der heuristischen Analyse als verdächtig erkannt. Im Augenblick des Funds enthalten die Antiviren-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
SUSP–	**Verdächtig**. Das Objekt enthält den modifizierten Code eines bekannten Virus. Die Desinfektion ist nicht möglich.	Das Programm hat erkannt, dass der Objektcode teilweise mit dem Code eines bekannten Virus übereinstimmt. Im Augenblick des Funds enthalten die Antiviren-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.

Präfix	Status des Objekts	Informationen zur Verarbeitung des Objekts
ERRO–	**Untersuchungsfehler**.	Bei der Untersuchung des Objekts ist ein Fehler aufgetreten. Das Programm erhält keinen Zugriff auf das Objekt: Die Integrität des Objekts ist beschädigt (z.B. kein Endpunkt in einem Multi-Level-Archiv) oder die Verbindung zu dem Objekt fehlt (wenn ein Objekt in einer Netzwerkressource untersucht wird). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
CURE–	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist möglich.	Das Objekt enthält einen Virus, der desinfiziert werden kann. Das Programm führt die Desinfektion des Objekts aus, wobei der Text des Viruskörpers in CURE geändert wird. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
DELE–	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.

Testen des Schutzes für HTTP-Datenverkehr

- *Gehen Sie folgendermaßen vor, um die den Virenschutz für den mit HTTP-Protokoll übertragenen Datenverkehr zu prüfen:*

  Versuchen Sie, den "Testvirus" von der offiziellen Internetseite des **EICAR**-Instituts herunterzuladen: http://www.eicar.org/anti_virus_test_file.htm.

Beim Versuch, den "Testvirus" herunterzuladen, erkennt Kaspersky Anti-Virus das Objekt, identifiziert es als infiziert und irreparabel, und führt die Aktion aus, die in den Einstellungen für die Untersuchung des HTTP-Datenverkehrs dafür festgelegt wurde. Wenn versucht wird, den "Testvirus" herunterzuladen, wird in der Grundeinstellung die Verbindung mit der Ressource getrennt und im Browserfenster erscheint eine Meldung darüber, dass dieses Objekt von dem Virus EICAR-Test-File infiziert ist.

Testen des Schutzes für SMTP-Datenverkehr

Um den Virenschutz für den mit SMTP-Protokoll übertragenen Datenverkehr zu prüfen, können Sie ein Mailprogramm verwenden, das die Daten mit diesem Protokoll überträgt.

> Hinweis
>
> Es wird empfohlen, die Arbeit der Anwendung für ausgehende E-Mail sowohl im Briefkörper als auch in Anlagen zu testen. Um den Virenschutz im Körper einer E-Mail zu prüfen, fügen Sie den Text des standardmäßigen oder modifizierten "Testvirus" in den Briefkörper ein.

- *Dazu:*

  1. Erstellen Sie mit Hilfe des auf Ihrem Computer installierten Mailprogramms eine E-Mail im Format **Gewöhnlicher Text**.

     > Hinweis
     >
     > Eine Nachricht, die den "Testvirus" enthält und das Format RTF oder HTML besitzt, wird nicht untersucht!

2. Fügen Sie den Text des standardmäßigen oder modifizierten "Testvirus" am Anfang der Nachricht ein oder hängen Sie eine Datei, die den "Testvirus" enthält, an die Nachricht an.
3. Schicken Sie die E-Mail an die Adresse des Administrators.

Das Programm erkennt das Objekt, identifiziert es als infiziert, blockiert das Senden von E-Mail.

ÜBERPRÜFUNG DER EINSTELLUNGEN VON DATEI-ANTI-VIRUS

- *Gehen Sie folgendermaßen vor, um zu prüfen, ob Datei-Anti-Virus korrekt eingestellt wurde:*

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen **EICAR**-Seite (http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.
2. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.
3. Starten Sie den "Testvirus" oder seine Modifikation zur Ausführung.

Datei-Anti-Virus fängt den Zugriff auf die Datei ab, untersucht sie und führt die in den Einstellungen festgelegte Aktion aus. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über die Arbeitsergebnisse von Datei-Anti-Virus sind im Bericht über die Arbeit der Komponente enthalten.

ÜBERPRÜFUNG DER EINSTELLUNGEN FÜR EINE AUFGABE ZUR VIRENSUCHE

- *Gehen Sie folgendermaßen vor, um zu prüfen, ob eine Aufgabe zur Virensuche korrekt eingestellt wurde:*

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen **EICAR**-Seite (http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen

"Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.

2. Erstellen Sie eine neue Untersuchungsaufgabe und wählen Sie als Untersuchungsobjekt den Ordner, der die "Testviren" enthält.
3. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.
4. Starten Sie die Ausführung der Aufgabe zur Virensuche.

Wenn bei der Untersuchung verdächtige oder infizierte Objekte gefunden werden, werden die in den Einstellungen der Aufgabe festgelegten Aktionen ausgeführt. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über das Ausführungsergebnis der Untersuchungsaufgabe sind im Bericht über die Arbeit der Komponente enthalten.

Überprüfung der Einstellungen für den Schutz vor unerwünschten E-Mails

Zur Überprüfung des Schutzes vor unerwünschten E-Mails können Sie eine Testnachricht verwenden, die vom Programm als Spam identifiziert wird.

Die Testnachricht muss folgenden Text in der Betreffzeile enthalten:

```
Spam is bad do not send it
```

Nachdem diese Nachricht auf dem Computer eintrifft, untersucht sie das Programm, weist ihr den Status Spam zu und führt die für ein Objekt mit diesem Status festgelegte Aktion aus.

ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

A. Einführung

Bitte lesen Sie dieses Dokument sorgfältig. Es enthält wichtige Informationen, die Sie kennen sollten, bevor Sie mit der Nutzung unserer Dienstleistungen oder Software fortfahren. Wenn Sie weiterhin Kaspersky Lab-Software oder –Dienste nutzen, wird davon ausgegangen, dass Sie diese Erklärung zur Datensammlung von Kaspersky Lab akzeptieren. Wir behalten uns das Recht vor, diese Erklärung zur Datensammlung jederzeit durch Veröffentlichung der Änderungen auf dieser Seite zu ändern. Bitte prüfen Sie das untenstehende Änderungsdatum, um festzustellen, ob der Inhalt sich geändert hat, seit Sie ihn zuletzt gelesen haben. Wenn Sie irgendeinen Teil der Kaspersky Lab-Dienste nach der Veröffentlichung der aktualisierten Erklärung zur Datensammlung nutzen, bedeutet dies, dass Sie mit den Änderungen einverstanden sind.

Kaspersky Lab und seine verbundenen Unternehmen (gemeinsam „Kaspersky Lab" genannt) haben diese Erklärung zur Datensammlung verfasst, um über ihre Vorgehensweise bei der Sammlung und Nutzung von Daten in Zusammenhang mit den Programmen Kaspersky Anti-Virus und Kaspersky Internet Security zu informieren und sie offenzulegen.

Vorbemerkung

Kaspersky Lab ist stets bestrebt, allen seinen Kunden hervorragenden Service zu bieten und insbesondere Ihre etwaigen Bedenken bezüglich der Sammlung von Daten zu beachten. Wir wissen, dass Sie vielleicht Fragen dazu haben, in welcher Weise Kaspersky Security Network Daten und Informationen sammelt und nutzt, und wir haben diese Erklärung („Erklärung zur Datensammlung" oder „Erklärung") verfasst, um Sie über die Grundsätze der Sammlung von Daten zu informieren, nach denen Kaspersky Security Network vorgeht.

Diese Erklärung enthält etliche allgemeine und technische Einzelheiten über die Maßnahmen, die wir unternehmen, um Ihre Bedenken bezüglich der Sammlung von Daten auszuräumen. Wir haben diese Erklärung in verschiedene Bereiche aufgeteilt, so dass Sie schnell und einfach die Information finden, die Sie gerade benötigen. Der Hauptgedanke ist, dass Ihre Wünsche und Erwartungen die Grundlage für alles bilden, was wir tun – einschließlich des Schutzes Ihrer Daten.

Die Angaben und Informationen wurden von Kaspersky Lab zusammengestellt und wenn Sie nach dem Studium dieser Erklärung noch Fragen oder Bedenken zum Datenschutz haben, schicken Sie bitte eine e-mail an support@kaspersky.com.

Was ist Kaspersky Security Network?

Das Kaspersky Security Network ermöglicht es weltweit allen Nutzern von Kaspersky Lab- Sicherheitsprodukten, dabei zu helfen, die Identifikation von neuen („in the Wild" auftretenden) Sicherheitsrisiken, die Ihren Computer bedrohen, zu erleichtern und die Zeit zu verkürzen, um einen Schutz dagegen zu entwickeln. Um neue Bedrohungen und ihre Ausgangspunkte zu identifizieren und um die Sicherheit der Nutzer und die Funktion der Produkte sicherzustellen, sammelt Kaspersky Security Network bestimmte Sicherheits- und Anwendungsdaten über mögliche Sicherheitsrisiken, die Ihren Computer im Visier haben und übermittelt diese Angaben zur Analyse an Kaspersky Lab. Diese Informationen enthalten keinerlei Angaben, die den Anwender persönlich identifizierbar machen, und sie werden von Kaspersky Lab ausschließlich benutzt, um die Sicherheit ihrer Produkte zu erhöhen und zukünftige Lösungen gegen Schadsoftware und Viren zu finden. Falls es im Einzelfall dennoch zu ungewollten Übertragungen von persönlichen Daten eines Anwenders kommen sollte, wird Kaspersky Lab diese streng nach den Vorgaben dieser Erklärung behandeln und schützen.

Indem Sie am Kaspersky Security Network teilnehmen, tragen Sie und die anderen Nutzer der Kaspersky Lab-Sicherheitsprodukte erheblich zu einem sichereren Internet bei.

Rechtliche Aspekte

Kaspersky Security Network unterliegt den Gesetzen verschiedener Rechtssysteme, weil seine Dienste in Ländern mit unterschiedlicher Gesetzgebung genutzt werden, einschließlich der Vereinigten Staaten von Amerika. Kaspersky Lab wird persönliche Daten auch ohne Ihre Erlaubnis offen legen, wenn dies durch Gesetz gefordert wird, oder im Guten Glauben, dass ein solches Vorgehen erforderlich ist, um schädigendes Verhalten gegen Gäste, Besucher und Mitarbeiter von Kaspersky Lab, sein Eigentum oder andere Rechtsgüter zu verfolgen oder davor zu schützen. Wie erwähnt, können sich Gesetze, die die von Kaspersky Lab gesammelten Daten und Informationen betreffen, von Land zu Land unterscheiden. Zum Beispiel unterliegen einige der gesammelten Daten und Informationen in der Europäischen Union und ihren Mitgliedstaaten den EU-Richtlinien über persönliche Daten, Privatsphäre und elektronische Kommunikation, einschließlich, aber nicht beschränkt auf die Richtlinie 2002/58/EC des Europäischen Parlamentes und des Ministerrates vom 12.07.2002 über die Behandlung von persönlichen Daten und den Schutz der Privatsphäre im Bereich der elektronischen Kommunikation und die Richtlinie 95/46/EC des Europäischen Parlamentes und des Ministerrates vom 24.10.1995 über den Schutz des Individuums unter Berücksichtigung der Verarbeitung von persönlichen Daten und über den freien Austausch solcher Daten und die daraus folgende Gesetzgebung in den Mitgliedstaaten der EU, sowie die Entscheidung

der Europäischen Kommission Nr. 497/2001/EC über allgemeine Vertragsbedingungen (betreffend die Übermittlung von persönlichen Daten an Drittstaaten) und die daraus folgende Gesetzgebung in den Mitgliedstaaten der EU.

Kaspersky Security Network wird die betroffenen Anwender informieren, wenn die oben erwähnten Informationen erstmalig gesammelt werden, ob diese Informationen weitergegeben werden, insbesondere zu geschäftlichen Zwecken, und wird diesen Internetnutzern die Möglichkeit geben, online der geschäftlichen Nutzung und der Weitergabe an Dritte entweder ausdrücklich zuzustimmen („opt-in“, in den Mitgliedstaaten der EU und anderen Ländern, die ein „opt-in“ verlangen) oder zu verlangen, dies zu unterlassen („opt-out“, in allen anderen Ländern).

Kaspersky Lab kann möglicherweise durch Gesetz oder durch die Justizbehörden aufgefordert werden, gewisse persönliche identifizierbare Daten bestimmten staatlichen Behörden offenzulegen. Wenn dies durch Gesetz oder Justizbehörden gefordert wird, werden wir diese Informationen gegen entsprechende Bestätigung herausgeben. Kaspersky Lab kann außerdem Informationen gegenüber der Justiz offen legen, um sein Eigentum sowie die Gesundheit und die Sicherheit von Personen zu schützen, soweit dies gesetzlich erlaubt ist.

Angaben zu den für den Datenschutz zuständigen Behörden der Mitgliedstaaten werden entsprechend der jeweils aktuellen Gesetzgebung der EU-Mitgliedstaaten gemacht. Informationen zu diesen Angaben sind im Servicebereich von Kaspersky Security Network verfügbar.

B. Gesammelte Informationen

Welche Daten wir sammeln

Der Kaspersky Security Network-Service sammelt grundlegende und weitergehende Daten über mögliche Sicherheitsrisiken, die Ihren Computer bedrohen, und gibt diese an Kaspersky Lab weiter. Die gesammelten Daten umfassen:

Grundlegende Daten

- Informationen über Ihre Hardware und Software, einschließlich Betriebssystem und installierte Service-Packs, Kernel-Objekte, Treiber, Dienstprogramme, Internet Explorer-Erweiterungen, Druckerweiterungen, Windows Explorer-Erweiterungen, heruntergeladene Programme, aktive Setup-Elemente, Ergänzungen der Taskleiste, Host- und Registry-Aufzeichnungen, IP-Adressen, Browsertyp, e-mail clients und die Versionsnummer des Kaspersky Lab-Produktes, diese lässt grundsätzlich keine persönliche Identifizierung zu.

- Eine individuelle ID, die vom Kaspersky Lab-Produkt zur Identifizierung bestimmter Maschinen erzeugt wird, ohne den Anwender zu identifizieren, und die keinerlei persönliche Informationen enthält.

- Informationen über den Stand des Schutzes vor Viren und Daten über alle Dateien oder Aktivitäten, die im Verdacht stehen, Malware zu sein (z.B. Virenname, Datum und Zeit der Entdeckung, Namen, Pfade und Größe der infizierten Dateien, IP und den Port einer Netzwerk-Attacke, Name der Anwendung, die im Verdacht steht, Malware zu sein). Bitte nehmen Sie zur Kenntnis, dass die erwähnten Daten keinerlei persönliche identifizierbare Informationen enthalten.

Weitergehende Daten

- Informationen über vom Nutzer heruntergeladene digital signierte Anwendungen (URL, Dateigröße, Name des Signierenden).
- Informationen über ausführbare Anwendungen (Größe, Attribute, Erstellungsdatum, Informationen zum PE-Header, Regionalcode, Name, Herkunft und benutzte Kompressionsmethode).

Sichern der Übertragung und der Aufbewahrung von Daten

Kaspersky Lab verpflichtet sich, die Sicherheit der gesammelten Informationen zu schützen. Die gesammelten Informationen werden auf Computer-Servern mit eingeschränktem und kontrolliertem Zugang gespeichert. Kaspersky Lab betreibt sichere Datennetzwerke, die durch Firewalls nach Industriestandard und durch passwortgeschützte Systeme geschützt sind. Kaspersky Lab nutzt umfangreiche Sicherheitstechnologien und Prozesse, um die gesammelten Informationen vor Bedrohungen durch unberechtigten Zugriff, Nutzung oder Offenlegung zu schützen. Unsere Sicherheitsrichtlinien werden regelmäßig überprüft und wenn nötig ergänzt, ausschließlich berechtigte Personen haben auf die gesammelten Daten Zugriff. Kaspersky Lab sorgt dafür, dass Ihre Informationen sicher und in Übereinstimmung mit dieser Erklärung behandelt werden. Bedauerlicherweise kann jedoch für keine Datenübertragung Sicherheit absolut garantiert werden. Daher können wir bei allem Bemühen, Ihre Daten zu schützen, nicht die Sicherheit aller Daten garantieren, die von Ihnen, unseren Produkten oder Diensten an uns übertragen werden, einschließlich, aber nicht darauf beschränkt, des Kaspersky Security Network. Sie nutzen alle diese Dienste auf Ihr eigenes Risiko.

Die gesammelten Daten werden an die Server von Kaspersky Lab übertragen und Kaspersky Lab hat die nötigen Vorsichtsmaßnahmen getroffen, um sicherzustellen, dass die gesammelten Informationen, wenn sie übertragen sind, auf einem angemessenen Niveau geschützt sind. Wir behandeln die von uns gesammelten Daten als vertraulich, sie unterliegen demzufolge unseren Sicherheitsmaßnahmen und unseren Richtlinien bezüglich des Schutzes und des Gebrauchs von vertraulichen Informationen. Wenn die gesammelten Daten Kaspersky Lab erreichen, werden sie auf einem Server gespeichert, der mit branchenüblichen Sicherheitsmaßnahmen versehen ist, einschließlich Nutzung von Login/Passwort-Verfahren und elektronischen Firewalls, die einen unberechtigten Zugriff von außerhalb verhindern. Vom Kaspersky Security Network gesammelte und unter diese Erklärung fallende Daten werden in den USA und ggf. unter weiteren Rechtssystemen erhoben und gespeichert, ebenso in anderen Staaten, in denen Kaspersky Lab tätig ist. Alle Mitarbeiter von

Kaspersky Lab beachten unsere Sicherheitsbestimmungen. Ihre Daten sind nur jenen Mitarbeitern zugänglich, die sie für ihre Arbeit benötigen. Keine gespeicherten Daten werden mit irgendeiner Information verbunden, die eine persönliche Identifikation ermöglicht. Kaspersky Lab vermischt die durch das Kaspersky Security Network gespeicherten Daten in keinem Fall mit Daten, Kontaktlisten oder vorgemerkten Informationen, die Kaspersky Lab für Werbung oder zu anderen Zwecken gesammelt hat.

C. Verwendung der gesammelten Daten

Wie Ihre persönlichen Informationen verwendet werden

Kaspersky Lab sammelt die Daten, um die Quellen von potentiellen Sicherheitsrisiken zu analysieren und zu identifizieren und die Fähigkeit von Kaspersky Lab-Produkten zu verbessern, verdächtiges Verhalten im Internet, betrügerische Websites, Crimeware und andere Arten von Sicherheitsbedrohungen im Internet aufzuspüren, um so auch zukünftig den bestmöglichen Schutz für die Kunden von Kaspersky Lab sicherzustellen.

Offenlegung von Informationen gegenüber Dritten

Kaspersky Lab kann jede der gesammelten Informationen offen legen, wenn es von einer Justizbehörde gefordert und aufgrund eine Gesetzes erlaubt oder gefordert ist oder aufgrund einer Vorladung oder eines anderen Rechtsinstrumentes, oder wenn wir in Gutem Glauben annehmen, dergestalt handeln zu müssen, um anwendbares Recht zu erfüllen, oder um einer Vorladung, einem anderen Rechtsinstrument oder einer durchsetzbaren staatlichen Anforderung zu entsprechen. Kaspersky Lab kann weiterhin persönliche Informationen, die Identifikationen zulassen, offen legen, wenn Grund zu der Annahme besteht, dass die Offenlegung dieser Information notwendig ist, um jemanden zu identifizieren, seiner habhaft zu werden oder rechtliche Mittel gegen ihn zu ermöglichen, der diese Erklärung oder die Inhalte Ihrer Vereinbarung mit uns verletzt haben könnte, oder um die Sicherheit unserer Nutzer und der Öffentlichkeit zu schützen, oder unter Beachtung von Geheimhaltungs- und Lizenzbestimmungen gegenüber Dritten, die uns bei Entwicklung, Betrieb und Wartung des Kaspersky Security Network unterstützen. Um die allgemeine Aufmerksamkeit sowie die Entdeckung von und die Vorbeugung vor Sicherheitsrisiken im Internet zu fördern, darf Kaspersky Lab bestimmte Informationen mit Forschungseinrichtungen und anderen Softwareanbietern teilen. Kaspersky Lab darf darüber hinaus Statistiken verwenden, die aus den gesammelten Informationen erstellt wurden, um Berichte über Entwicklungen von Sicherheitsrisiken zu erstellen und zu veröffentlichen.

Ihre Wahlmöglichkeiten

Die Teilnahme am Kaspersky Security Network ist optional. Sie können das Kaspersky Security Network jederzeit aktivieren bzw. deaktivieren, indem Sie die Feedback-Einstellungen unter den „Optionen“ Ihres Kaspersky-Produktes aufsuchen. Bitte beachten Sie jedoch, wenn Sie sich entschließen, angeforderte Informationen oder Daten zurückzuhalten, dass wir Sie in diesem Fall nicht mit

einigen Leistungen versorgen können, die von der Sammlung dieser Daten abhängig sind. Wenn die Wartungsperiode Ihres Kaspersky Lab-Produktes abläuft, kann es sein, dass einige Funktionen der Software weiterhin zur Verfügung stehen, aber es werden keine Informationen mehr automatisch an Kaspersky Lab gesendet.

Wir behalten aus außerdem das Recht vor, unregelmäßige Alarmmeldungen an die Nutzer zu senden, um sie über spezifische Änderungen zu informieren, die ihre Fähigkeit zur Nutzung unserer Dienste, für die sie sich entschieden haben, beeinflussen können. Wir behalten uns weiterhin das Recht vor, Sie zu kontaktieren, wenn es aus rechtlichen Gründen notwendig ist oder wenn eine Verletzung einer gültigen Lizenz, Garantie oder Verkaufsbestimmung vorliegt.

Kaspersky Lab behält sich diese Rechte vor, weil wir in einzelnen Fällen der Meinung sind, das Recht zu benötigen, mit Ihnen in Kontakt zu treten, sei es aus rechtlichen Gründen oder aus sonstigen Gründen, die für Sie wichtig sein können. Diese Rechte erlauben uns jedoch nicht, Sie anzusprechen, um neue oder auch bestehende Dienstleistungen zu bewerben, wenn Sie uns dies nicht gestattet haben, und die Anlässe für diese Arten der Kommunikation sind in der Praxis selten.

D. Datensammlung – Weitere Fragen und Beschwerden

Kaspersky Lab behandelt die Bedenken seiner Nutzer bezglich der Datensammlung mit uerstem Respekt und Aufmerksamkeit. Wenn Sie mit einem Punkt dieser Erklrung in Bezug auf Ihre Informationen oder Daten nicht einverstanden sind oder wenn Sie andere Fragen oder Beschwerden haben, schreiben Sie uns oder kontaktieren Sie Kaspersky Lab per e-mail: support@kaspersky.com.

Beschreiben Sie in Ihrer Nachricht bitte so genau wie möglich den Grund Ihrer Nachfrage. Wir werden Ihrer Frage oder Beschwerde unverzüglich nachgehen.

Die Bereitstellung von Informationen ist freiwillig. Die Option der Datensammlung kann vom Anwender jederzeit im Bereich „Feedback“ auf der Seite „Einstellungen“ des entsprechenden Kaspersky-Produktes abgeschaltet werden.

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Die Zentrale befindet sich in Russland, es gibt Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Benelux-Ländern, China, Polen, Rumänien und in den USA (Kalifornien). In Frankreich wurde eine neue Tochtergesellschaft gegründet, das Europäische Zentrum für Antiviren-Forschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das ist heute mehr als vierhundertfünfzig hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome, sechzehn einen Doktortitel haben. Die führenden Virusanalytiker von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens sind das einzigartige Wissen und die Erfahren, die die Mitarbeiter im Laufe des mehr als vierzehnjährigen ununterbrochenen Kampfes gegen Viren gesammelt haben. Dank der ständigen Analyse von Virenaktivitäten können wir Tendenzen bei der Malware-Entwicklung vorhersagen und frühzeitig Benutzern einen zuverlässigen Schutz vor neuen Angriffen an die Hand geben. Dieser Vorteil manifestiert sich in den Erzeugnissen und Leistungen von Kaspersky Lab. Wir sind unseren Wettbewerbern stets einen Schritt voraus und bieten unseren Kunden den besten Schutz.

Aufgrund der jahrelangen Tätigkeit wurde das Unternehmen zum führenden Entwickler von Technologien zum Schutz vor Viren. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus® und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Bequeme Steuerelemente versetzen die Benutzer in die Lage, den Antivirenschutz von Computern und Unternehmensnetzwerken maximal zu automatisieren. Viele westeuropäische Developer verwendeten in ihrer Software den Kernel von Kaspersky Anti-Virus ®, beispielsweise: Nokia ICG (USA), F-Secure (Finnland), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir projektieren, realisieren und begleiten Antiviren-Komplex-Lösungen von Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Wir haben für unsere Benutzer einen rund um die Uhr erreichbaren technischen Kundendienst in mehreren Sprachen eingerichtet.

In diesem Abschnitt

Andere Produkte von Kaspersky Lab 77
Unsere Kontaktinformationen 87

Andere Produkte von Kaspersky Lab

Kaspersky Lab News Agent

Das Programm News Agent dient der schnellen Zustellung der Nachrichten von Kaspersky Lab, der Benachrichtigung über das "Virus-Wetter" und über neu erschienene Nachrichten. Das Programm liest in vorgegebenen Zeitabständen von den Kaspersky-Lab-Newsservern eine Liste der verfügbaren Nachrichtenkanäle und der darin enthaltenen Informationen.

News Agent verfügt außerdem über folgende Funktionen:

- Visualisierung des Zustands des "Viren-Wetters" im Infobereich der Taskleiste
- Abonnieren und Abbestellen der Nachrichtenkanäle von Kaspersky Lab
- Download von Nachrichten für jeden abonnierten Kanal in festgelegten Zeitabständen. Außerdem erfolgt eine Benachrichtigung über ungelesene Nachrichten
- Anzeige von Nachrichten der abonnierten Kanäle
- Anzeige einer Liste der Kanäle und ihrer Status
- Öffnen der Webseite mit dem vollständigen Nachrichtentext im Browser

News Agent funktioniert unter dem Betriebssystem Microsoft Windows. Er kann als separates Programm benutzt werden oder zu unterschiedlichen integrierten Lösungen von Kaspersky Lab gehören.

Kaspersky® OnLine Scanner

Dieses Programm ist ein kostenloser Dienst, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antiviren-Untersuchung des Computers im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Browser ausgeführt. Dadurch kann der Benutzer schnell eine Antwort auf Fragen erhalten, die mit einer Infektion durch schädliche Programme verbunden sind. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- Standardmäßige oder erweiterte Datenbanken für die Untersuchung wählen.
- Die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

Kaspersky® OnLine Scanner Pro

Dieses Programm stellt einen Abonnementsdienst dar, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antiviren-Untersuchung des Computers und die Desinfektion infizierter Dateien im Online-Modus erlaubt. Kaspersky OnLine Scanner Pro wird direkt im Browser ausgeführt. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- Standardmäßige oder erweiterte Datenbanken für die Untersuchung wählen.
- Gefundene infizierte Objekte desinfizieren.
- Die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

Kaspersky Anti-Virus® Mobile

Kaspersky Anti-Virus Mobile gewährleistet den Schutz für mobile Geräte, die mit den Betriebssystemen Symbian OS und Microsoft Windows Mobile arbeiten. Das Programm erlaubt die komplexe Antiviren-Untersuchung und umfasst:

- Scan auf Befehl des Arbeitsspeichers, der Speicherkarten, eines einzelnen Ordners oder einer konkreten Datei des mobilen Geräts Bei einem Fund wird das infizierte Objekt isoliert oder gelöscht.

- Echtzeitschutz: Alle eingehenden oder veränderten Objekte werden automatisch untersucht. Außerdem werden Dateien beim Zugriff untersucht.
- Schutz vor SMS- und MMS-Spam.

Kaspersky Anti-Virus for Mail-Server

Das Produkt schützt die Dateisysteme von Servern, die unter den Betriebssystemen Microsoft Windows, Novell NetWare, Linux und Samba laufen, zuverlässig vor allen Arten schädlicher Programme. Das Produkt umfasst folgende Anwendungen von Kaspersky Lab:

- Kaspersky Administration Kit
- Kaspersky Anti-Virus for Windows Server
- Kaspersky Anti-Virus for Linux File Server
- Kaspersky Anti-Virus for Novell Netware
- Kaspersky Anti-Virus for Samba Server

Vorzüge und Funktionen:

- Echtzeitschutz der Dateisysteme von Servern: alle Dateien der Server werden untersucht, wenn versucht wird, sie zu öffnen und auf dem Server zu speichern.
- Verhinderung von Viren-Epidemien.
- Scan auf Befehl des gesamten Dateisystems oder bestimmter Ordner und Dateien.
- Einsatz von Optimierungstechnologien bei der Untersuchung von Objekten des Serverdateisystems.
- Systemwiederherstellung nach einer Infektion.
- Skalierbarkeit der Software im Rahmen der verfügbaren Systemressourcen.
- Berücksichtigung der Systemauslastung.
- Verwendung einer Liste mit vertrauenswürdigen Prozessen, deren Aktivität auf dem Server nicht vom Programm kontrolliert wird.
- Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung.
- Speicherung von Sicherungskopien infizierter und gelöschter Objekte, um sie bei Bedarf wiederherzustellen.

- Isolierung verdächtiger Objekte in einem speziellen Speicher.
- Benachrichtigungen über Ereignisse bei der Arbeit des Produkts für den Systemadministrator.
- Ausführliche Berichtsführung.
- Automatisches Update der Datenbanken des Softwareprodukts.

Kaspersky Open Space Security

Kaspersky Open Space Security realisiert eine neue Art des Herangehens an die Sicherheit moderner Unternehmensnetzwerke mit beliebigem Umfang. Dabei gewährleistet es den zentralen Schutz von Informationssystemen und unterstützt externe Arbeitsplätze und mobile Benutzer.

Das Softwareprodukt umfasst vier Produkte:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Im Folgenden wird jedes Produkt genau beschrieben.

Kaspersky Work Space Security bietet den zentralen Schutz von Workstations innerhalb und außerhalb eines Unternehmensnetzwerks. Es schützt vor allen aktuellen Internet-Bedrohungen wie Viren, Spyware, Hackerangriffen und Spam: Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam.

Vorzüge und Funktionen:

- Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam
- Proaktiver Schutz vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden
- Personal Firewall mit IDS/IPS-System
- Rollback-Funktion für schädliche Veränderungen im System
- Schutz vor Phishing-Angriffen und Spam
- Dynamisches Ressourcen-Management bei der vollständigen Untersuchung des Systems
- Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung

- Unterstützung von Cisco® NAC (Network Admission Control)
- Untersuchung von E-Mails und Internet-Traffic in Echtzeit
- Sperren von Popupfenstern und Werbebannern bei der Arbeit im Internet
- Sichere Arbeit in Netzwerken aller Art einschließlich WiFi
- Tools zum Erstellen einer Notfall-CD zur Systemwiederherstellung, um die Folgen von Virenangriffen zu beheben
- Flexibles Informationssystem für den Schutzstatus
- Automatisches Update der Datenbanken
- Vollständige Unterstützung von 64-Bit-Betriebssystemen
- Optimiert für Notebooks mit Intel® Centrino®
- Möglichkeit zur Remote-Reparatur (Intel® Active Management, Intel® vPro™)

Kaspersky Business Space Security bietet den optimalen Schutz für die Informationsressourcen einer Firma vor Internet-Bedrohungen. Kaspersky Business Space Security schützt Workstations und Dateiserver vor allen Arten von Viren, trojanischen Programmen und Würmern, verhindert Viren-Epidemien und gewährleistet zusätzlich die Integrität von Informationen und den unverzögerten Zugriff von Benutzern auf Netzwerkressourcen.

Vorzüge und Funktionen:

- Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- Unterstützung von Cisco® NAC (Network Admission Control)
- Schutz von Workstations und Dateiservern vor allen Internet-Bedrohungen
- Verwendung der iSwift-Technologie zur Vermeidung wiederholter Untersuchungen innerhalb eines Netzwerks
- Dynamische Auslastung der Serverprozessoren
- Isolierung verdächtiger Objekte von Workstations in einem speziellen Speicher
- Rollback-Funktion für schädliche Veränderungen im System

- Skalierbarkeit der Software im Rahmen der verfügbaren Systemressourcen
- Proaktiver Schutz vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden
- Untersuchung von E-Mails und Internet-Traffic in Echtzeit
- Personal Firewall mit IDS/IPS-System
- Schutz bei der Arbeit in drahtlosen WiFi-Netzwerken
- Technologie zum Selbstschutz des Antiviren-Programms vor Schadprogrammen
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Automatisches Update der Datenbanken

Kaspersky Enterprise Space Security

Das Produkt umfasst Komponenten zum Schutz von Workstations und Groupware-Servern vor allen aktuellen Internet-Gefahren. Viren werden aus dem E-Mail-Datenstrom gelöscht. Die Integrität der Daten sowie die schnelle und sichere Verfügbarkeit der Netzwerkressourcen werden gewährleistet.

Vorzüge und Funktionen:

- Schutz für Workstations und Server vor Viren, Trojanern und Würmern
- Schutz der Mailserver Sendmail, Qmail, Postfix und Exim
- Untersuchung aller E-Mails auf einem Microsoft Exchange Server einschließlich der gemeinsamen Ordner
- Verarbeitung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern
- Schutz vor Phishing-Angriffen und Spam
- Verhinderung von massenhaften E-Mails und Viren-Epidemien
- Skalierbarkeit der Software im Rahmen der verfügbaren Systemressourcen
- Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- Unterstützung von Cisco® NAC (Network Admission Control)

- Proaktiver Schutz vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden
- Personal Firewall mit IDS/IPS-System
- Schutz bei der Arbeit in drahtlosen WiFi-Netzwerken
- Untersuchung des Internet-Traffics in Echtzeit
- Rollback-Funktion für schädliche Veränderungen im System
- Dynamisches Ressourcen-Management bei der vollständigen Untersuchung des Systems
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Berichtssystem für den Schutzstatus
- Automatisches Update der Datenbanken

Kaspersky Total Space Security

Diese Lösung überwacht alle ein- und ausgehenden Datenströme, E-Mails, Internet-Traffic und alle Netzwerkaktionen. Kaspersky Total Space Security umfasst Komponenten zum Schutz von Workstations und mobilen Geräten, gewährleistet den schnellen und sicheren Zugriff der Anwender auf die Informationsressourcen der Firma und auf das Internet. Außerdem garantiert es Sicherheit bei der Kommunikation per E-Mail.

Vorzüge und Funktionen:

- Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam auf allen Ebenen eines Unternehmensnetzwerks von der Workstation bis zur Internet-Gateway
- Proaktiver Schutz vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden
- Schutz für Mailserver und Groupware-Server
- Echtzeit-Untersuchung des Internet-Datenverkehrs (HTTP/FTP), der in ein lokales Netzwerk eintrifft
- Skalierbarkeit der Software im Rahmen der verfügbaren Systemressourcen
- Sperren des Zugriffs auf infizierte Workstations
- Verhinderung von Viren-Epidemien
- Zentrale Berichte über den Schutzstatus

- Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- Unterstützung von Cisco® NAC (Network Admission Control)
- Unterstützung von Hardware-Proxyservern
- Filterung des Internet-Datenverkehrs nach einer Liste vertrauenswürdiger Server, nach Objekttypen und nach Benutzergruppen
- Verwendung der iSwift-Technologie zur Vermeidung wiederholter Untersuchungen innerhalb eines Netzwerks
- Dynamisches Ressourcen-Management bei der vollständigen Untersuchung des Systems
- Personal Firewall mit IDS/IPS-System
- Sichere Arbeit in Netzwerken aller Art einschließlich WiFi
- Schutz vor Phishing-Angriffen und Spam
- Möglichkeit zur Remote-Reparatur (Intel® Active Management, Intel® vPro™)
- Rollback-Funktion für schädliche Veränderungen im System
- Technologie zum Selbstschutz des Antiviren-Programms vor Schadprogrammen
- Vollständige Unterstützung von 64-Bit-Betriebssystemen
- Automatisches Update der Datenbanken

Kaspersky Security für Mail-Server

Kaspersky Security für Mail-Server schützt Mailserver und Groupware-Server gegen Schadprogramme und Spam. Das Produkt umfasst Anwendungen für den Schutz aller bekannten Mailserver wie Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix und Exim. Zudem kann auch ein separater Mail-Gateway organisiert werden. Zu dieser Lösung gehören:

- Kaspersky Administration Kit
- Kaspersky Mail Gateway
- Kaspersky Anti-Virus for Lotus Notes/Domino
- Kaspersky Anti-Virus for Microsoft Exchange
- Kaspersky Anti-Virus for Linux File Server

Funktionen:

- Zuverlässiger Schutz vor schädlichen und potenziell gefährlichen Programmen
- Spam-Filterung
- *Scan von ein- und ausgehenden E-Mails und E-Mail-Anhängen*
- Untersuchung aller E-Mails auf einem Microsoft Exchange Server einschließlich der gemeinsamen Ordner
- Untersuchung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern
- Filterung von E-Mails nach Typen der Anhänge
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Komfortable Bedienung
- Verhinderung von Viren-Epidemien
- Monitoring für den Status des Schutzsystems mit Hilfe von Benachrichtigungen
- Berichtssystem über die Arbeit der Anwendung
- Skalierbarkeit der Software im Rahmen der verfügbaren Systemressourcen
- Automatisches Update der Datenbanken

Kaspersky Security für Internet-Gateway

Das Produkt gewährleistet allen Mitarbeitern eines Unternehmens den sicheren Zugriff auf das Internet. Die Lösung löscht automatisch alle schädlichen und potenziell gefährlichen Programme aus dem Datenstrom, der über die Protokolle HTTP und FTP eintrifft. Das Produkt umfasst:

- Kaspersky Administration Kit
- Kaspersky Anti-Virus for Proxy Server
- Kaspersky Anti-Virus for Microsoft ISA Server
- Kaspersky Anti-Virus for Check Point FireWall-1

Funktionen:

- Zuverlässiger Schutz vor schädlichen und potenziell gefährlichen Programmen

- Untersuchung des Internet-Traffics (HTTP/FTP) in Echtzeit
- Filterung des Internet-Datenverkehrs nach einer Liste vertrauenswürdiger Server, nach Objekttypen und nach Benutzergruppen
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Komfortable Bedienung
- Berichtssystem über die Arbeit der Anwendung
- Unterstützung von Hardware-Proxyservern
- Skalierbarkeit der Software im Rahmen der verfügbaren Systemressourcen
- Automatisches Update der Datenbanken

Kaspersky® Anti-Spam

Kaspersky Anti-Spam ist die erste in Russland entwickelte Software zum Spam-Schutz von kleinen und mittleren Unternehmen. Das Programm vereint moderne Verfahren der Sprachanalyse für Informationen in Textform, sämtliche modernen Verfahren zum Filtern von E-Mails (einschließlich RBL-Listen und formeller Prüfung von Nachrichten) sowie eine einmalige Auswahl an Dienstprogrammen, durch die der Nutzer in die Lage versetzt wird, bis zu 95 % der unerwünschten Nachrichten zu identifizieren und zu eliminieren.

Kaspersky® Anti-Spam ist ein Filterprogramm, das, am "Eingang" des firmeninternen Netzwerks installiert, sämtliche eingehenden E-Mails auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mailing-System und kann sowohl auf bereits funktionierenden als auch auf separaten Mailservern installiert werden.

Die tägliche Aktualisierung der Filterdatenbank mit Mustertexten aus unserem Sprachlabor garantiert eine hohe Effizienz des Produkts. Die Datenbank-Updates erscheinen alle 20 Minuten.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper bietet Höchstgeschwindigkeit bei der Antiviren-Untersuchung des Datenverkehrs auf Servern, die Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web verwenden.

Das Programm besitzt die Form eines Plug-ins (Erweiterungsmoduls) und führt im Echtzeit-Modus die Antiviren-Untersuchung und die Verarbeitung der ein- und ausgehenden E-Mail-Nachrichten durch.

UNSERE KONTAKTINFORMATIONEN

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie am Telefon oder per E-Mail gerne umfassend beraten. Alle Ihre Fragen werden vollständig und ausführlich beantwortet.

Anschrift:	Steinheilstrasse 13, D-85053 Ingolstadt, Deutschland
Telefon, Fax:	Tel.: +49 (0) 841 98 18 90 (Montags bis Freitags von 9 bis 17 Uhr) Fax: +49 (0) 841 98 189 100
Technischer Support:	http://support.kaspersky.com/de/
Webforum von Kaspersky Lab	http://forum.kaspersky.com
Antiviren-Labor:	newvirus@kaspersky.com (nur für die Einsendung von neuen Viren in Archiv-Form)
Feedback zu unseren Benutzerhandbüchern:	docfeedback@kaspersky.com (Diese Adresse ist für Rückmeldungen über das Handbuch und das elektronische Hilfesystem gedacht)
Allgemeine Informationen:	http://www.kaspersky.de info@kaspersky.com
Internet:	http://www.kaspersky.de http://www.viruslist.de

MOZILLA FOUNDATION

Bei der Entwicklung von Komponenten der Anwendung wurde folgende Bibliothek verwendet: **Gecko SDK Version 1.8.**

Diese Software wird nach den Bedingungen der Lizenz MPL 1.1 http://www.mozilla.opg/MPL verwendet.

Ausführliche Informationen über die Bibliothek **Gecko SDK** finden Sie unter folgender Adresse: http://developer.mozilla.org/en/docs/Gecko_SDK.

Webseite der Mozilla Foundation:
http://www.mozilla.org

ENDBENUTZER-LIZENZVERTRAG FÜR DIE ERWORBENE KASPERSKY LAB SOFTWARE

WICHTIG – bitte sorgfältig lesen: Lesen Sie die in diesem KASPERSKY LAB Endbenutzer-Lizenzvertrag ("EULA") beschriebenen Rechte und Einschränkungen sorgfältig durch. Sie werden gebeten, die Bestimmungen des EULAs zu prüfen und ihnen zuzustimmen oder diese abzulehnen.

Indem Sie das Sicherheitsetikett auf der CD-Box aufreißen oder wenn Sie die SOFTWARE installieren, erklären Sie sich mit den Bestimmungen des EULAs einverstanden. Falls Sie mit den Bestimmungen des EULAs NICHT einverstanden sind, geben Sie die erworbene Software bitte innerhalb von 14 Tagen an die Einkaufsstelle zurück. Nach Eingabe des Aktivierungscodes ist eine Rückgabe der Software ausgeschlossen.

Jede Bezugnahme auf "Software" schließt den Aktivierungscode oder die Schlüsseldatei ein, den Sie von Kaspersky Lab als Teil der Software erhalten.

Dieser EULA ist ein rechtsgültiger Vertrag zwischen Ihnen, dem Besitzer eines Exemplars der SOFTWARE (entweder als natürlicher oder als juristischer Person) und KASPERSKY LAB. KASPERSKY LAB wird sich das exklusive Urheberrecht auf die Computersoftware (auf die Software und die Antiviren-Datenbanken) vorbehalten. Indem Sie die SOFTWARE installieren, erklären Sie sich damit einverstanden, durch die Bestimmungen dieses EULAs gebunden zu sein. Falls Sie den Bestimmungen dieses EULAs nicht zustimmen, sind Sie nicht berechtigt, die SOFTWARE zu installieren und zu verwenden.

Die SOFTWARE ist sowohl durch Urheberrechtsgesetze und internationale Urheberrechtsverträge als auch durch andere Gesetze und Vereinbarungen über geistiges Eigentum geschützt.

1. LIZENZEINRÄUMUNG. Durch diesen EULA werden Ihnen folgende Rechte eingeräumt:

- Sie sind berechtigt, eine Kopie der SOFTWARE auf einem einzigen Computer zu installieren und zu verwenden. Eine Mehrplatzlizenz der SOFTWARE, dürfen Sie auf so vielen Computern installieren, wie Sie Lizenzen erworben haben.

- Sie sind berechtigt, die installierte SOFTWARE gemäß den Bestimmungen dieses Vertrags zu benutzen. Das Recht, Aktualisierungen (Updates) der SOFTWARE zu beziehen, besteht nur, wenn sie es mit dem Verkäufer der SOFTWARE vereinbart haben und nur für die vereinbarte Dauer. Wenn Sie aufgrund Kaufvertrags oder in sonstiger Weise berechtigt sind, Aktualisierungen zu beziehen, so gelten die Bestimmungen dieses Vertrags entsprechend für die aktualisierte SOFTWARE. Sie können diesen Vertrag jederzeit kündigen, indem Sie alle Kopien der Software und der Dokumentation zerstören.

2. EINSCHRÄNKUNGEN

- Einschränkungen im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung. Sie sind nicht berechtigt, die SOFTWARE zurückzuentwickeln (Reverse Engineering), zu dekompilieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung, dies ausdrücklich gestattet. Sie sind nicht berechtigt, diese Software in automatischen, halbautomatischen oder manuellen Tools zu verwenden, welche dazu dienen, Virensignaturen, Virenerkennungsroutinen, sowie beliebige andere Daten oder Codes zum Erkennen von schädlichem Code oder Daten zu erstellen.

- Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.

- Supportleistungen. Nach Kauf und Aktivierung der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die beim Kauf der SOFTWARE oder unabhängig davon vereinbarte Dauer. Supportleistungen verstehen sich wie folgt:

  - stündliche Updates der Antiviren-Datenbank
  - kostenloses Updates der Software
  - technische Unterstützung sowohl per e-Mail als auch per Telefon mit KASPERSKY LAB

3. KÜNDIGUNG. Unbeschadet sonstiger Rechte ist KASPERSKY LAB berechtigt, diesen EULA fristlos zu kündigen, sofern Sie gegen die Bestimmungen dieses EULAs verstoßen. In einem solchen Fall sind Sie verpflichtet, sämtliche Kopien der SOFTWARE und alle ihre Komponenten zu vernichten.

4. URHEBERRECHT. Das Urheberrecht auf die Software, die gedruckten Begleitmaterialien und jede Kopie der Software liegt bei Kaspersky Lab, soweit es durch die Veräußerung nicht erschöpft ist.

5. GEWÄHRLEISTUNG. Kaufvertragliche Gewährleistungsansprüche bestehen nur gegenüber dem Unternehmen oder der Person, von der Sie die Software gekauft haben. Mit diesem Lizenzvertrag ist keine Erweiterung der kaufrechtlichen Gewährleistung verbunden. Nur für den Fall, dass Sie die Software unmittelbar von Kaspersky Lab gekauft haben sollten, gilt: KASPERSKY LAB gewährleistet, dass:

- die SOFTWARE den Spezifikationen im wesentlichen entspricht.
- Im Falle einer physikalischen Lieferung der Originaldatenträger frei von Material- und Herstellungsfehlern ist.
- Das Programm korrekt auf den Datenträger aufgezeichnet ist, die Dokumentation sämtliche Informationen enthält, die KASPERSKY LAB für die Benutzung der Software für erforderlich hält.
- Die SOFTWARE binnen 90 Tagen ab der ersten Installation oder dem ersten Download, falls richtig behandelt, der in der beiliegenden Dokumentation bestimmten Funktionalität entspricht und laut derer voll funktionsfähig ist.

Gewährleistungspflichtige Mängel werden von KASPERSKY LAB oder dessen Lieferanten nach Entdeckung, auf jeden Fall aber vor Ablauf von der Gewährleistungsfrist, dem Ermessen von Kaspersky Lab nach, durch Ersatz, Reparatur, Umtausch oder Rückzahlung beseitigt, falls eine Mangelrüge rechtzeitig an Kaspersky Lab oder dessen Lieferanten gerichtet wurde. KASPERSKY LAB oder dessen Lieferanten übernehmen keine Gewährleistung für Mängel, die auf andere als für die Software vorgesehenen Einsatzbedingungen, unsachgemäße Behandlung oder dergleichen zurückzuführen sind.

ALLE ANDERE GEWÄHRLEISTUNGEN UND BEDINGUNGEN, SEIEN SIE AUSDRÜCKLICH ODER KONKLUDENT, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF, (FALLS ZUTREFFEND) JEDE KONKLUDENTE GEWÄHRLEISTUNG IM HINBLICK AUF HANDELSÜBLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, FAHRLÄSSIGKEIT ODER MANGELNDE FACHMÄNNISCHE BEMÜHUNGEN WERDEN VON KASPERSKY LAB ODER DESSEN LIEFERANTEN ABGELEHNT. ES BESTEHT EBENFALLS KEINE GEWÄHRLEISTUNG ODER BEDINGUNG VON RECHTSANSPRÜCHEN IN BEZUG AUF RECHTSINHABERSCHAFT, UNGESTÖRTES NUTZUNGVERGNÜGEN ODER NICHTVERLETZUNG VON RECHTEN DRITTER. DAS GESAMTE RISIKO, DAS BEI DER BENUTZUNG ODER LEISTUNG DER SOFTWARE ENTSTEHT, LIEGT BEI IHNEN.

6. AUSSCHLUSS DER HAFTUNG FÜR ALLE SCHÄDEN. SOWEIT GESETZLICH ZUGELASSEN, SIND KASPERSKY LAB ODER DESSEN LIEFERANTEN IN KEINEM FALL HAFTBAR FÜR IRGENDWELCHE FOLGE-,

ZUFÄLLIGEN, DIREKTEN, INDIREKTEN, SPEZIELLEN, STRAFRECHTLICHEN ODER ANDEREN SCHÄDEN WELCHER ART AUCH IMMER (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AN PERSONEN ODER SACHEN, SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG, VERLUST VON GESCHÄFTLICHEN INFORMATIONEN, FÜR DEN VERLUST VON PRIVATSPHÄRE, DIE UNMÖGLICHKEIT, EINE PFLICHT ZU ERFÜLLEN (EINSCHLIESSLICH GEMÄSS TREU UND GUTEN GLAUBENS ODER VERNÜNFTIGER ANGEMESSENER SORGFALT) ZU ERFÜLLEN, FÜR FAHRLÄSSIGKEIT ODER ANDERE VERMÖGENSSCHÄDEN), DIE AUS DER VERWENDUNG DER SOFTWARE ODER DER TATSACHE, DASS SIE NICHT VERWENDET WERDEN KANN, RESULTIEREN ODER DAMIT IN ZUSAMMENHANG STEHEN, SELBST WENN KASPERSKY LAB ODER DESSEN LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WORDEN IST. DIESER HAFTUNGSAUSSCHLUSS FÜR SCHÄDEN GILT AUCH DANN, WENN ABHILFEMASSNAHMEN IHREN WESENTLICHEN ZWECK VERFEHLEN.

7. ANWENDBARES RECHT. Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Die Geltung des UN-Kaufrechts ist ausgeschlossen.